

【特許請求の範囲】

【請求項 1】 マルチパスが存在するカットスルーパスの設定に際し、自装置が関与するカットスルーパスの設定状況に関する全部または所定の一部の情報に基づいて、次段ルータとし得る複数のルータ装置のうちから負荷分散に寄与するようにルータ装置を選択し、この選択されたルータ装置を次段ルータとするカットスルーパスの設定のための所定の制御を行うことを特徴とするカットスルーパス制御方法。

【請求項 2】 ある宛先のためのカットスルーパスを設定する際に、次段ルータとなり得るルータ装置が複数存在する場合、宛先を同じくする既設定のカットスルーパス数に基づいて、該次段ルータとなり得る各ルータ装置へのカットスルーパス数が均等的に配分されるように、該設定すべきカットスルーパスにおいて次段ルータとするルータ装置を選択することを特徴とするカットスルーパス制御方法。

【請求項 3】 ある整数値を、前記宛先のためのカットスルーパスにおける次段ルータとなり得るルータ装置の数で除したときに出現し得る、0 から始まる各剰余の値夫々を、該次段ルータとなり得るルータ装置に 1 つずつ割り当てておき、前記選択の際、前記既設定のカットスルーパス数を前記ルータ装置の数で除して得られた剰余の値に対して割り当てられたルータ装置を選択することを特徴とする請求項 2 に記載のカットスルーパス制御方法。

【請求項 4】 ある宛先のためのカットスルーパスを設定する際に、次段ルータとなり得るルータ装置が複数存在する場合、宛先を同じくする既設定のカットスルーパス数に基づいて、該次段ルータとなり得る各ルータ装置へのカットスルーパス数が各ルータ装置に対するリンク速度に応じて公平に配分されるように、該設定すべきカットスルーパスにおいて次段ルータとする次段ルータとするルータ装置を選択することを特徴とするカットスルーパス制御方法。

【請求項 5】 ある整数値を、前記宛先のためのカットスルーパスにおける次段ルータとなり得る各ルータ装置に対するリンク速度の比を表すもしくは近似する整数比の各要素の総和で除したときに出現し得る、0 から始まる各剰余の値夫々を、該次段ルータとなり得るルータ装置に、前記リンク速度に応じた個数ずつ割り当てておき、前記選択の際、前記既設定のカットスルーパス数を前記整数比の各要素の総和で除して得られた剰余の値に対して割り当てられたルータ装置を選択することを特徴とする請求項 4 に記載のカットスルーパス制御方法。

【請求項 6】 前記選択されたルータ装置に前記カットスルーパスを設定するためのメッセージを送出し、前記カットスルーパスが設定されたならば、該カットスルーパスを利用するための情報設定を行うことを特徴とする請求項 1 ないし 6 のいずれか 1 項に記載のカットス

ルーパス制御方法。

【請求項 7】 前記選択されたルータ装置への他の既設定のカットスルーパスが未だ存在しない場合には、前記選択したルータ装置に前記カットスルーパスを設定するためのメッセージを送出し、該カットスルーパスが設定されたならば、該カットスルーパスを利用するための情報設定を行い、

前記選択されたルータ装置への他の既設定のカットスルーパスが既に存在する場合には、該既に設定されているカットスルーパスに該設定すべきカットスルーパスをマージするための情報設定を行うことを特徴とする請求項 1 ないし 6 のいずれか 1 項に記載のカットスルーパス制御方法。

【請求項 8】 前記カットスルーパスの設定は、上流側のノード装置からカットスルーパスを設定するためのメッセージを受信したことを契機として開始することを特徴とする請求項 1 ないし 7 のいずれか 1 項に記載のカットスルーパス制御方法。

【請求項 9】 所定のタイミングで、自装置からのカットスルーパスの次段ノードとなっている各ノード装置へのトラフィック量を調べ、

前記各ノード装置へのトラフィック量の不均衡状態が、予め規定された許容範囲を越えている場合には、トラフィック量のより少ない方のノード装置を次段ノードとしているマルチパスの存在するカットスルーパスであって該トラフィック量に関する所定の条件を満足するものを選択し、

この選択したカットスルーパスの次段ノードを、トラフィック量の多い方のノード装置に設定変更することを特徴とする請求項 1 ないし 8 のいずれか 1 項に記載のカットスルーパス制御方法。

【請求項 10】 前記選択および設定変更を、前記不均衡状態が前記許容範囲内に収まるまで、または前記選択ができなくなるまで、繰り返し行うことを特徴とする請求項 9 に記載のカットスルーパス制御方法。

【請求項 11】 前記選択において、最適な 1 または複数のカットスルーパスの解を求めることを特徴とする請求項 9 に記載のカットスルーパス制御方法。

【請求項 12】 自装置が関与するカットスルーパスのトラフィック状況に関する全部または所定の一部の情報に基づいて、自装置において経路変更可能なカットスルーパスのうち経路変更した場合に負荷分散に寄与するものを選択し、

この選択されたカットスルーパスの経路を、負荷分散に寄与するように経路変更することを特徴とするカットスルーパス制御方法。

【請求項 13】 マルチパスが存在するカットスルーパスを設定する際に、自装置が関与するカットスルーパスの設定状況に関する全部または所定の一部の情報に基づいて、次段ルータとし得る複数のルータ装置のうちから

負荷分散に寄与するようにルータ装置を選択する手段と、
この選択されたルータ装置を次段ルータとするカットスルーパスの設定のための所定の制御を行う手段とを具備したことを特徴とするルータ装置。

【請求項 14】 自装置が関与するカットスルーパスのトラフィック状況に関する全部または所定の一部の情報に基づいて、自装置において経路変更可能なカットスルーパスのうち経路変更した場合に負荷分散に寄与するものを選択する手段と、

この選択されたカットスルーパスの経路を、負荷分散に寄与するように経路変更する手段とを具備したことを特徴とするルータ装置。

【請求項 15】 プライベートアドレス空間から成るプライベートネットワークに接続されパケットを転送する手段を有するプライベート処理モジュールと、非プライベートアドレス空間から成る非プライベートネットワークに接続されパケットをラベルスイッチする手段を有する非プライベート処理モジュールと、を備えるシステムにおける通信方法であって、

前記非プライベート処理モジュールは、前記プライベート処理モジュールが接続されたプライベートネットワークと前記プライベートアドレス空間を共有する他のプライベートネットワークを収容する他のシステムが前記非プライベートネットワークに存在することを認識した場合に、当該他のシステムへ向けて前記非プライベートネットワークを経由するラベルスイッチパスを設定するためのプロトコル通信を行い、

前記非プライベート処理モジュールは、設定された前記ラベルスイッチパスを前記プライベート処理モジュールまで延長し、前記プライベート処理モジュールに前記他のシステムのプライベートアドレスを通知し、

前記プライベート処理モジュールは、前記他のシステムのプライベートアドレス宛のパケットを、延長された前記ラベルスイッチパスへ転送することを特徴とする通信方法。

【請求項 16】 前記プライベート処理モジュールと前記非プライベート処理モジュールとの間に予め複数のパスを用意しておき、前記ラベルスイッチパスの延長は、この複数のパスから選択した一つのパスと、設定された前記ラベルスイッチングパスとを、前記非プライベート処理モジュール内で対応付けることにより行い、前記他のシステムのプライベートアドレスは、選択された前記一つのパスと対応付けて通知されることを特徴とする請求項 15 に記載の通信方法。

【請求項 17】 前記ラベルスイッチパスの延長は、前記ラベルスイッチパスが前記他のシステムに到達するように設定されたことが確認された後に行うことを特徴とする請求項 15 に記載の通信方法。

【請求項 18】 前記他のシステムのプライベートアドレ

スの通知は、パケットを前記他のシステムへ運ぶための前記ラベルスイッチと、パケットを前記他のシステムから運ぶための別のラベルスイッチとの双方が設定された場合に行うことを特徴とする請求項 15 に記載の通信方法。

【請求項 19】 前記システムは、前記プライベートアドレス空間とは異なるプライベートアドレス空間から成る第二のプライベートネットワークに接続されパケットを転送する手段を有する第二のプライベート処理モジュールをも備えるものであり、

前記非プライベート処理モジュールは、前記第二のプライベート処理モジュールが接続された第二のプライベートネットワークと前記異なるプライベートアドレス空間を共有する他の第二のプライベートネットワークを収容する他のシステムが前記非プライベートネットワークに存在することを認識した場合にも、当該他のシステムへ向けて前記非プライベートネットワークを経由するラベルスイッチパスを設定するためのプロトコル通信を行い、

20 前記非プライベート処理モジュールは、設定された前記ラベルスイッチパスを前記第二のプライベート処理モジュールまで延長し、前記第二のプライベート処理モジュールに前記他のシステムのプライベートアドレスを通知し、

前記第二のプライベート処理モジュールは、前記他のシステムのプライベートアドレス宛のパケットを、延長された前記ラベルスイッチパスへ転送することを特徴とする請求項 15 に記載の通信方法。

【請求項 20】 ラベルスイッチパスをその内部に設定可能なラベルスイッチネットワークと、それ以外の非ラベルスイッチネットワークとを含み、プライベートアドレス空間を共有する少なくとも二つのプライベートネットワークの間に位置する非プライベートネットワークにおいて、仮想的なプライベートネットワークを構成するための通信方法であって、

前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータが、前記プライベートネットワークの一方から当該ルータへのラベルスイッチパスを設定するのに用いられた制御メッセージの内容に基づき、該ラベルスイッチパスから受信したパケットの宛先プライベートアドレスが前記プライベートネットワークの他方であることを認識し、受信した該パケットを前記プライベートネットワークの他方に対応する非プライベートアドレスでカプセル化して送信することを特徴とする通信方法。

【請求項 21】 前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータが、前記プライベートネットワークの一方から当該ルータへのラベルスイッチパスを設定するのに用いられた制御メッセージの内容に基づき、自身が前記プライベート

5

ートネットワークの境界ルータであると前記非プライベートネットワーク内に広告し、

前記プライベートネットワークの他方を収容する前記非プライベートネットワークに接続されたルータは、この広告に基づいて前記プライベートネットワークの他方からのパケットを前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータの非プライベートアドレスでカプセル化して送信し、

このカプセル化されたパケットを受信した前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータは、該カプセル化を解いて該パケットを当該ルータから前記プライベートネットワークの一方へのラベルスイッチバスへ送信することを特徴とする請求項 20 に記載の通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、カットスルーバスを設定するルータ装置及びカットスルーバス制御方法並びにラベルスイッチ機能を有するルータ装置の通信方法に関する。

【0002】

【従来の技術】IP（インターネットプロトコル）ヘッダを解析することによりデータグラムを転送するルータ装置では、次の転送先を決めるためにルーチングプロトコルを使用している。その一つとして使用されている OSPF（Open Shortest Path Fast；例えば、J. Moy, "OSPF Version 2", Internet RFC 2328, April 1998 参照）等では、最終宛先ネットワークまたはホストまでの同一のコストの経路について、次の転送先が複数存在する場合には、次の転送先情報を複数保持することが可能である。ここで、コストとは例えば途中経由するルータ数などの情報であり、コストが低い場合に最短経路で到着することを意味する。

【0003】この機能は負荷分散（ロードバランス）などで使用し、例えば、転送するルータ装置で、複数の次の転送先ルータ情報を持つ場合には、それぞれについて均一に出力することで、片方のルータ装置だけが高負荷にならないようにしている。ここで、注意すべき点は、ロードバランス時には、2 ホスト間のデータ転送において、データグラムの順序が逆転しないようにすることが必要である。

【0004】一方、IP 等のデータグラム転送を高速化するための一手法として考案されているラベルスイッチの技術では、データグラム転送中には IP ヘッダ情報を見ないため、2 ホスト間のデータ転送におけるデータグラムの順序保証は困難である。

【0005】そこで、現在は IP ヘッダによる転送を行う装置（ここでは、エッジルータと呼ぶ）から、複数の

6

カットスルー転送を行うためのバス（ラベルスイッチバスと呼ぶ）を設定し、エッジルータで複数設定したカットスルーバスのいずれかにデータグラムを転送するという手法が取られる。

【0006】この手法におけるラベルスイッチバス設定としては、エッジルータから設定を開始するときに、各バスを強制的に通るような設定（Explicit Route）が存在する。

【0007】Explicit Route による設定の場合、途中のルータ装置での経路変更による、指定した経路（ルータ装置）が削除された場合等において、必ずエッジルータが認識する必要があり、指定された経路が削除されたことを検出したルータからエッジルータに対し通知する際に、ルーチングプロトコルもしくはカットスルーを生成するためのプロトコル情報を使用する等、特別な手段が必要とされる場合がある。

【0008】また、従来の方では、自身には複数の経路を持たない場合でも、複数経路を認識する必要があり、ルーチングプロトコルによっては困難な場合があり、ネットワーク管理者がネットワーク設計時に登録しなければならない可能性がある。

【0009】

【発明が解決しようとする課題】以上のように従来、カットスルーバスに関するロードバランスを実行する場合、ロードバランスのために経路変更する該当カットスルーバスのエッジルータがこれに関与する必要があるという問題点があった。また、このために、制御や実装が複雑になる、効果的なロードバランスの実現が難しい、などの不具合があった。

【0010】本発明は、上記事情を考慮してなされたもので、ロードバランスを実行する場合に、実際にマルチバス情報を持つルータ装置にて行い、エッジルータにて特別な処理が必要とならないようにしたカットスルーバス制御方法及びルータ装置を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明（請求項 1）に係るカットスルーバス制御方法は、マルチバスが存在するカットスルーバスの設定に際し、自装置が関与するカットスルーバスの設定状況に関する全部または所定の一部の情報（例えば、設定しようとしているカットスルーバスと宛先を同じくする既設定のカットスルーバス数、選択し得る各ルータ装置に対するリンク速度）に基づいて、次段ルータとし得る複数のルータ装置のうちから負荷分散に寄与するようにルータ装置を選択し、この選択されたルータ装置を次段ルータとするカットスルーバスの設定のための所定の制御を行うことを特徴とする。

【0012】ここで、ルータ装置とは、IP などのネットワーク層の経路表を持つもののことを言うものとする。

【0013】なお、負荷分散に寄与するようにルータ装置を選択する手順としては、その時点で最も負荷分散に寄与するルータ装置があるならばそれを選択するような手順だけでなく、一定のスパンで見ても負荷分散させるような手順をも意味する。簡単な例を示すと、例えば、次段ルータとし得る3つのルータ装置（ルータ1、ルータ2、ルータ3）について、ルータ1、2、3、1、2、3、…の順番に選択することになるような手順が前者に該当し、ルータ1、1、2、2、3、3、1、1、2、2、3、3、…の順番に選択することになるような手順が後者に該当する。

【0014】また、負荷分散は、宛先を同じくするマルチパスで設定されたカットスルーパスの範囲毎に行っても良いし、全カットスルーパスに渡って行っても良いし、また、その他にも種々の方法が考えられる。

【0015】また、種々のファクターを考慮してより実効的な負荷分散を実現するようにしてもよい。

【0016】本発明（請求項2）に係るカットスルーパス制御方法は、ある宛先のためのカットスルーパスを設定する際に、次段ルータとなり得るルータ装置が複数存在する場合、宛先を同じくする（この場合、次段ルータとなり得る複数のルータ装置が同じになる）既設定のカットスルーパス数に基づいて、該次段ルータとなり得る各ルータ装置へのカットスルーパス数が均等的に配分されるように、該設定すべきカットスルーパスにおいて次段ルータとするルータ装置を選択することを特徴とする。

【0017】なお、前述と同様、均等的に配分されるようにルータ装置を選択する手順としては、その時点で最も均等化に寄与するルータ装置があるならばそれを選択するような手順だけでなく、一定のスパンで見ても均等化させるような手順をも意味する。

【0018】また、好ましくは、ある整数値を、前記宛先のためのカットスルーパスにおける次段ルータとなり得るルータ装置の数で除したときに出現し得る、0から始まる各剰余の値々々を、該次段ルータとなり得るルータ装置に1つずつ割り当てておき、前記選択の際、前記既設定のカットスルーパス数を前記ルータ装置の数で除して得られた剰余の値に対して割り当てられたルータ装置を選択するようにしてもよい。簡単な例を示すと、例えば、次段ルータとし得る2つのルータ装置（ルータ1、ルータ2）について、剰余が0の場合にはルータ1を選択し、剰余が1の場合にはルータ2を選択するものとする、ルータ1、2、1、2、…の順番に選択することになる。

【0019】本発明（請求項4）に係るカットスルーパス制御方法は、ある宛先のためのカットスルーパスを設定する際に、次段ルータとなり得るルータ装置が複数存在する場合、宛先を同じくする（この場合、次段ルータとなり得る複数のルータ装置が同じになる）既設定のカ

ットスルーパス数に基づいて、該次段ルータとなり得る各ルータ装置へのカットスルーパス数が各ルータ装置に対するリンク速度に応じて公平に配分されるように、該設定すべきカットスルーパスにおいて次段ルータとする次段ルータとするルータ装置を選択することを特徴とする。

【0020】なお、前述と同様、各ルータ装置に対するリンク速度に応じて公平に配分されるようにルータ装置を選択する手順としては、その時点で最も公平化に寄与するルータ装置があるならばそれを選択するような手順だけでなく、一定のスパンで見ても公平化させるような手順をも意味する。

【0021】また、好ましくは、ある整数値を、前記宛先のためのカットスルーパスにおける次段ルータとなり得る各ルータ装置に対するリンク速度の比を表すもしくはは近似する整数比の各要素の総和で除したときに出現し得る、0から始まる各剰余の値々々を、該次段ルータとなり得るルータ装置に、前記リンク速度に応じた個数ずつ割り当てておき、前記選択の際、前記既設定のカットスルーパス数を前記整数比の各要素の総和で除して得られた剰余の値に対して割り当てられたルータ装置を選択するようにしてもよい。簡単な例を示すと、例えば、次段ルータとし得る3つのルータ装置（ルータ1、ルータ2、ルータ3）について、ルータ1に対するリンク速度：ルータ2に対するリンク速度：ルータ3に対するリンク速度＝1：2：3とすると、剰余が0、3または5の場合にはルータ3を選択し、剰余が1または4の場合にはルータ2を選択し、剰余が2の場合にはルータ1を選択するものとする、ルータ3、2、1、3、2、3、3、2、1、3、2、3、…の順番に選択することになる。また、剰余が0、1または2の場合にはルータ3を選択し、剰余が3または4の場合にはルータ2を選択し、剰余が5の場合にはルータ1を選択するものとして、ルータ3、3、3、2、2、1、3、3、3、2、2、1、…の順番に選択するようにすることもできる。

【0022】さらに、以上の各構成において、好ましくは、前記選択されたルータ装置に前記カットスルーパスを設定するためのメッセージを送出し、前記カットスルーパスが設定されたならば、該カットスルーパスを利用するための情報設定を行うようにしてもよい。これは、マージを行わない場合である。

【0023】あるいは、好ましくは、前記選択されたルータ装置への他の既設定のカットスルーパスが未だ存在しない場合には、前記選択したルータ装置に前記カットスルーパスを設定するためのメッセージを送出し、該カットスルーパスが設定されたならば、該カットスルーパスを利用するための情報設定を行い、前記選択されたルータ装置への他の既設定のカットスルーパスが既に存在する場合には、該既に設定されているカットスルーパスに該設定すべきカットスルーパスをマージするための情報

10

20

30

40

50

設定を行うようにしてもよい。これは、マージを行う場合である。

【0024】以上において、好ましくは、前記カットスルーパスの設定は、上流側のノード装置からカットスルーパスを設定するためのメッセージを受信したことを契機として開始するようにしてもよい。

【0025】また、以上において、好ましくは、所定のタイミング（例えば、一定間隔で周期的に、何らかのイベントが発生したことを契機として、など）で、自装置からのカットスルーパスの次段ノードとなっている各ノード装置へのトラフィック量を調べ、前記各ノード装置へのトラフィック量の不均衡状態が、予め規定された許容範囲を越えている場合には、トラフィック量のより少ない方のノード装置を次段ノードとしているマルチパスの存在するカットスルーパスであって該トラフィック量に関する所定の条件を満足するもの（例えば、そのカットスルーパスの経路を設定変更したことによってトラフィック量の多いノード装置と少ないノード装置の関係を逆転させないもの、そのカットスルーパスの経路を設定変更したことによって前記不均衡状態が前記許容範囲内に収まることになるようなもの、など）を選択し、この選択したカットスルーパスの次段ノードを、トラフィック量の多い方のノード装置に設定変更するようにしてもよい。

【0026】この場合に、好ましくは、前記選択および設定変更を、前記不均衡状態が前記許容範囲内に収まるまで、または前記選択ができなくなるまで、繰り返し行うようにしてもよい。

【0027】あるいは、好ましくは、前記選択において、最適な1または複数のカットスルーパスの解を求め

【0028】本発明（請求項12）に係るカットスルーパス制御方法は、自装置が関与するカットスルーパスのトラフィック状況に関する全部または所定の一部の情報に基づいて、自装置において経路変更可能なカットスルーパスのうち経路変更した場合に負荷分散に寄与するものを選択し、この選択されたカットスルーパスの経路を、負荷分散に寄与するように経路変更するようにしてもよい。

【0029】本発明（請求項13）に係るルータ装置は、マルチパスが存在するカットスルーパスを設定するに際し、自装置が関与するカットスルーパスの設定状況に関する全部または所定の一部の情報に基づいて、次段ルータとし得る複数のルータ装置のうちから負荷分散に寄与するようにルータ装置を選択する手段と、この選択されたルータ装置を次段ルータとするカットスルーパスの設定のための所定の制御を行う手段とを具備したことを特徴とする。

【0030】本発明（請求項14）に係るルータ装置は、自装置が関与するカットスルーパスのトラフィック

状況に関する全部または所定の一部の情報に基づいて、自装置において経路変更可能なカットスルーパスのうち経路変更した場合に負荷分散に寄与するものを選択する手段と、この選択されたカットスルーパスの経路を、負荷分散に寄与するように経路変更する手段とを具備したことを特徴とする。

【0031】本発明によれば、ロードバランスを実行する場合に、エッジルータの関与なしに、実際にマルチパス情報を持つルータ装置のみに行うことができる。

【0032】また、制御や実装の複雑化を回避し、効果的なロードバランスを実現することができる。

【0033】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0034】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0035】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0036】図1は、ラベルスイッチを導入したネットワークであってルータ装置が次段情報を複数持ち得るようなネットワークの一例を示すものである。

【0037】ルータ装置101～103は、各ルータ間にて、転送するデータグラムフローの情報と下位レイヤの情報について共通の認識を得ることで、IPヘッダ情報を見ることなく、下位レイヤ情報だけに基づいて高速にデータグラム転送を行うことを可能とするパス（以下、カットスルーパスと呼ぶ）を生成する機能を有する装置である。

【0038】特定のデータグラムの情報と下位レイヤ情報（以下、ラベルと呼ぶ）について共通の認識を得る手段としては、例えば、FANP（Flow Attribute Notification Protocol）、TDP（Tag Distribution Protocol）、LDP（Label Distribution Protocol）等のプロトコルが用いられる。

【0039】ルータ装置104は、ルータ装置102、103やその先のネットワーク120と接続される装置であり、ルータ装置102およびルータ装置103との間でFANP、TDP、LDP等のプロトコルが動作しており、カットスルーパスの設定やカットスルーパスの最終段としての機能を有する。

【0040】ルータ装置111～11Nは、ルータ装置101と接続され、ルータ装置104と同様に、FAN

P、TDP、LDP等のプロトコルが動作しており、カットスループスの設定やカットスループスの最終段としての機能を有する。

【0041】なお、上記のように各ルータ装置101～103/104/111～11Nについて（以下の説明のために便宜的に）区別をしたが、全てのルータ装置がカットスルー転送機能を有するようなものであっても構わない。

【0042】図1のネットワークでは、各ルータ間において、IPデータグラムの転送先を決定するルーチングプロトコルが動作しており、動作しているプロトコルとしては、OSPF（Open Shortest Path Fast）等が考えられる。

【0043】ネットワーク上でルーチングプロトコルを動作させることにより、ルータ装置101では、ネットワーク120やルータ装置104にデータグラムを転送する場合に、ルータ装置102を経由するルートとルータ装置103を経由するルートのいずれを採用しても同一のコストで到達可能であることを認識することができる。これによって、ルータ装置101では、データグラム転送時にルータ装置102とルータ装置103のどちらに転送しても良いことになる。

【0044】このような構成において、ルータ装置111～11Nから、ネットワーク120またはルータ装置104に対し、FANP、TDP、LDP等のプロトコルを用いた、カットスループス131～13Nを生成する場合について説明する。

【0045】この場合、ルータ装置101では、ルータ装置111～11Nからそれぞれ到着した設定メッセージを、ルータ装置104またはネットワーク120の方向に向かって転送することになるが、ルータ装置101では、データグラムを転送する場合と同様に、カットスルーを延長するためにメッセージを転送する次のルータ装置として、ルータ装置102とルータ装置103のどちらに転送しても良いことになる。

【0046】ここで、図2に、図1に例示したようなネットワーク構成内に存在するルータ装置101の一構成例を示す。なお、これと同一の構成をルータ装置102やルータ装置103が持っても良いが、図1のネットワーク構成例ではルータ装置101のみマルチパスを持つため、このルータ装置101を例としている。

【0047】IP処理部201は、IPデータグラムの宛先情報に基づいて当該データグラムが自分宛のものである否か調べ、自分宛のデータグラムについては、受信処理を行って、上位のプロトコル（例えば、TCP）に転送し、自分宛でないものについては、次の転送先を決定し、次段のルータ装置に転送するための処理を行う。

【0048】なお、ルータ装置101では、ラベルによるスイッチング機能を有するため、後者の自分宛でないデータグラムに対する転送機能を有する必要性は必ず

しもない。ただし、ルータ装置104やルータ装置111～11Nが図1の構成を取る場合には、これらについては、カットスルーの始点および終点となり得るため、データグラムの転送機能は必要となる。

【0049】カットスルー制御部202は、隣接するルータ装置との間でデータグラムフローおよびラベル情報について共通の認識を得る（データグラムフローとラベルの情報をやり取りする）ために使用するプロトコルを実行する部分である。

10 【0050】ルーチングテーブル203は、宛先アドレスから次に送るべきルータ装置を求めるためのテーブルであり、次段情報は複数持つことも可能であるが、経路によってはマルチパスが存在しない場合もあるので、必ずしも複数ではない。

【0051】ネットワークインタフェース211～21Nは、それぞれルータ装置111～11Nと接続されるもので、物理層としては、FANP、TDP、LDP等が使用可能なものであれば、どのようなものでも良い。例えば、ATM、フレームリレー、イーサネットなどが

20 【0052】ネットワークインタフェース221は、ルータ装置102に接続され、動作としてはネットワークインタフェース211～21Nと同様のものである（ここでは、ネットワークインタフェース211～21Nと同一構成とする）。

【0053】ネットワークインタフェース222は、ルータ装置103に接続され、動作としてはネットワークインタフェース211～21Nと同様のものである（ここでは、ネットワークインタフェース211～21Nと同一構成とする）。

【0054】スイッチ部204は、カットスルー転送が可能な場合には、ネットワークインタフェースからネットワークインタフェースへと直接スイッチング可能となるようなスイッチ装置である。

【0055】各ネットワークインタフェースの構成について、ネットワークインタフェース211を例にとって説明する。

【0056】物理層処理部231は、ネットワークインタフェースが収容する物理層に応じて異なる処理が行われるが、ATMの場合にはセル同期等の処理、イーサネットの場合にはMAC処理等が、物理層処理にあたる。

【0057】ラベル処理部232は、受信したデータグラム（フレーム）のヘッダ情報よりラベルを抽出した後、ラベルテーブル233を検索することで、次のルータ装置へのラベルを決定し、IPヘッダ等を使用したデータグラム転送処理を実行せずに、スイッチ部204を通じてそのまま次のルータに転送するための処理を行うものである。

【0058】なお、ATMの場合には、ラベル処理部232およびラベルテーブル233は、ATMスイッチ等

で使用するVPI/VCIによるスイッチテーブルがそのまま使用可能であり、ルータ装置101が保有するネットワークインタフェースが全てATMの場合には、ネットワークインタフェース211~21N、221、222、ラベル処理部232、ラベルテーブル233、スイッチ部204の全ての機能がATMスイッチで実現可能となる。

【0059】以下では、ルータ装置101のカットスルーパス設定手順について説明する。

【0060】図3に、図1に例示したネットワークにおいてルータ装置111~11Nから最終宛先をネットワーク120またはルータ装置104とするカットスルーパスの生成を行ったような場合における、ルータ装置101の処理手順の一例を示す。ここでは、マージを行わない場合の例について説明する。

【0061】なお、カットスループロトコル生成用のプロトコルによって動作は異なるが、ここでは、カットスルー生成用のメッセージ（以下、設定メッセージと呼ぶ）を契機に次段のルータにメッセージを転送する場合の一例について説明する。

【0062】ルータ装置101のネットワークインタフェース211~21Nより受信したカットスルーパス生成用のメッセージは、ラベル処理部232にてラベルテーブル223検索後、直接他のネットワークインタフェースに転送せずに、IP等のデータグラム処理を行う旨を決定し、IP処理部201に転送する（ステップS301）。

【0063】なお、データグラム処理を行うための条件は各プロトコルによって異なるが、基本的にスイッチ部204にてIP処理部201に対し転送する処理を行う点は同様である。

【0064】設定メッセージを転送されたIP処理部201では、自身が受信すべきメッセージがどうかの判断を行い、カットスループロトコル用のメッセージの場合には、カットスルー制御部202にデータが送られる（ステップS302）。

【0065】一方、IP処理部201にて自身で受信すべきメッセージでないと判断した場合には、IP転送処理を行うことになり、IP処理部201は、ルーティングテーブル203を検索した後、次のルータ装置を決定し、次のルータ装置にデータを転送する（ステップS303）。なお、このとき、ルータ装置101にてIP転送機能を有さないような装置構成の場合には、データグラムは廃棄される。

【0066】さて、IP処理部201より設定メッセージを受信したカットスルー制御部202では、受信メッセージ中に含まれるカットスルーパスを生成するための最終宛先を獲得する（ステップS304）。

【0067】カットスルー制御部202では、獲得した最終宛先からルーティングテーブル203を検索して、次

段のルータ装置を求め（ステップS305）、最終宛先が到達不能の場合には、そのメッセージの転送は停止される（ステップS306）。

【0068】なお、メッセージの転送が停止された後の動作は、カットスルー生成プロトコルによって異なり、ルータ装置101から前段のルータ装置111~11Nに対し、応答（以下、応答メッセージを設定完了メッセージと呼ぶ）を返すものや、そのままプロトコル動作を停止しておくものが存在する。

10 【0069】一方、ステップS305にて最終宛先が存在する場合には、そのルーティングテーブル203のエントリより、次段のルータ装置の情報を獲得する。

【0070】図1のネットワーク例では既に述べたように、ルータ装置101において、ルータ装置104およびネットワーク120に対しては、ルータ装置102およびルータ装置103が次段情報として保持されている。

20 【0071】このとき、カットスルー制御部202では、同一最終宛先に対し、既に設定されているカットスルーパスの本数（カットスルー数）を確認する（ステップS307）。

【0072】設定済みカットスルー数は、次段情報を求めるための判断に使用し、例えば、図1のネットワーク構成のように、次段情報が2つ存在する場合には、設定済みカットスルー数が0および偶数のときにはルータ装置102を選択し、奇数のときには、ルータ装置103を選択するようなアルゴリズムにより、次段情報が決定される（ステップS308）。

30 【0073】なお、次段情報がn存在する場合には、設定済みカットスルー数をcとすると、例えば、 $c \bmod n$ の値に基づいて、各次段ルータ装置を順番に選択していけばよい。

【0074】また、この次段ルータ装置選択アルゴリズムは上記のものに限らず、各次段ルータ装置が同一（もしくはほぼ同一）のパス数に設定される、あるいはパスが各次段ルータ装置に均等に配分される、ようにする方法であれば、どのようなものでも良い。

【0075】このようにして次段ルータを決定したカットスルー制御部202では、次段ルータ装置がルータ装置102と決定された場合にはネットワークインタフェース221を通じてルータ装置102に、また、ルータ装置103と決定された場合にはネットワークインタフェース222を通じてルータ装置103に、該設定メッセージを送出する（ステップS309）。

40 【0076】この後、カットスルーの終点であるルータ装置104もしくは途中のルータより、設定完了メッセージが到着した時点で（ステップS310）、受信したメッセージ中に含まれるフロー情報とラベル情報とそれに対応する送信フロー情報とラベル情報の関連付けが完了し、入力インタフェース上211~211N上から出

カインタフェース 221 または出カインタフェース 222 へのカットスルーパスの設定が可能となり、カットスルー転送への移行が可能となる（ステップ S311）。

【0077】カットスルー転送への移行は、図2のような構成のルータ装置の場合には、受信インタフェース 211～21N 上に存在するラベルスイッチテーブル 233 上に、出カラベル情報を設定することで完了となる。

【0078】カットスルー転送への移行が完了となったときに、カットスルー制御部 202 では、設定完了メッセージを前段のルータ装置に転送する。

【0079】このように次段ルータを決定する手順において、既に設定されたカットスルーパスの本数を参考に同一（もしくはほぼ同一）の本数となるようにすることで、パスレベルのロードバランスを取ることが可能となる。

【0080】次に、図2に示したルータ装置 101 について、スイッチ部 204 にて複数の入力ラベルを一つの出カラベルに送出可能なマージ機能をサポートしている場合について説明する。

【0081】図4に、ルータ装置 101 がマージ機能を有する（マージを行う）場合において、例えばルータ装置 111～11N が最終宛先をネットワーク 120 またはルータ装置 104 とするような、カットスルーパスの生成時における、ルータ装置 101 の処理手順の一例を示す。

【0082】ルータ装置 101 のネットワークインタフェース 211～21N より受信したカットスルーパス生成用のメッセージは、ラベル処理部 232 にてラベルテーブル 223 検索後、直接他のネットワークインタフェースに転送せずに、IP 等のデータグラム処理を行う旨を決定し、IP 処理部 201 に転送する（ステップ S401）。

【0083】なお、データグラム処理を行うための条件は各プロトコルによって異なるが、基本的にスイッチ部 204 にて IP 処理部 201 に対し転送する処理を行う点は同様である。

【0084】設定メッセージを転送された IP 処理部 201 では、自身が受信すべきメッセージがどうかの判断を行い、カットスループロトコル用のメッセージの場合には、カットスルー制御部 202 にデータが送られる（ステップ S402）。

【0085】一方、IP 処理部 201 にて自身で受信すべきメッセージでないと判断した場合には、IP 等のデータグラム転送処理を行うが、このときに、IP 処理部 201 は、ルーティングテーブル 203 を検索した後、次のルータ装置を決定し、次のルータ装置にデータを転送する（ステップ S403）。なお、このとき、ルータ装置 101 にてデータグラム転送機能を有さない場合には、データを廃棄しても構わない。

【0086】さて、IP 処理部 201 より設定メッセー

ジを受信したカットスルー制御部 202 では、メッセージ中に含まれるカットスルーパスを生成するための最終宛先を獲得する（ステップ S404）。

【0087】メッセージより獲得した最終宛先からルーティングテーブル 203 を検索して、次段のルータ装置を求める（ステップ S405）。最終宛先が到達不能の場合には、そのメッセージの転送は停止される（ステップ S406）。

【0088】なお、メッセージの転送が停止された後の動作は、カットスルー生成プロトコルによって異なり、ルータ装置 101 から前段のルータ装置 111～11N に対し、応答を返すものや、そのままプロトコル動作を停止しておくものが存在する。

【0089】一方、ステップ S405 にて最終宛先が存在する場合には、そのルーティングテーブル 203 のエントリより次段のルータ装置の情報を獲得可能であり、図1のルータ装置 101 の場合には、既に述べたようにルータ装置 104 およびネットワーク 120 に対してはルータ装置 102 およびルータ装置 103 が次段情報として保持されている。

【0090】カットスルー制御部 202 では、次段ルータ装置を選択することになるが、このときに、同一最終宛先に対し、既に設定されているカットスルーパスの本数を確認する（ステップ S407）。

【0091】設定済みカットスルー数は、次段情報を求めるための判断に使用し、図3に示した場合と同様に、例えば、設定済みカットスルー数が0および偶数の場合にはルータ装置 102 を選択し、奇数の場合には、ルータ装置 103 を選択するようなアルゴリズムにより、次段情報が決定される（ステップ S408）。前述と同様に、このアルゴリズムは上記のものに限らず、各次段ルータ装置が同一パス数に設定されるなどの方法であれば、どのようなものでも良い。

【0092】次に、設定済みカットスルー数が保持される次段情報よりも少ない場合、すなわち本例では設定済みカットスルー数が0本および1本の場合には、まだカットスルーパスが最大数（本例では2本）生成されていないため、決定された次段ルータに対し、設定メッセージが送出される（ステップ S409）。

【0093】この後、カットスルーの終点であるルータ装置 104 もしくは途中のルータからの設定完了のメッセージが到着することで（ステップ S410）、受信したメッセージ中に含まれるフロー情報とラベル情報とそれに対応する送信フロー情報とラベル情報の関連付けが完了し、入力インタフェース上 211～211N 上から出カインタフェース 221 または 222 へのカットスルーパスの設定が可能となり、カットスルー転送への移行が可能となる（ステップ S411）。

【0094】カットスルー転送への移行は、図2のような構成のルータ装置の場合には、受信インタフェース 2

11~21N上に存在するラベルスイッチテーブル233上に、出力ラベル情報を設定することで完了となる。

【0095】また、設定済みカットスルー数が保持される次段情報の個数以上の場合、すなわち本例では設定済みカットスルー数が2本以上の場合には、既に送出すべきカットスルーパスはそれぞれの次段ルータとの間で設定されており、カットスルー制御部202では、決定された次段ルータ情報に対し、設定されたカットスルーパスにマージして送出するように、受信した設定メッセージの入カインタフェース上211~211N上のラベル

スイッチテーブルに設定することで完了する(ステップS411)。

【0096】この後、設定メッセージを送出してきたルータ装置に対し、設定完了メッセージを応答する。

【0097】なお、このようにマージを行う場合には、ステップS408の次段情報の決定において、全ての次段情報が1回ずつ選択されるまでは、1つの次段情報が複数回選択されないようにするのが好ましい(上記で示した例では、そのようになっている)。ただし、選択基準を緩やかにして、全ての次段情報が1回ずつ選択されるまでに、1つの次段情報が複数回選択されても構わないようにすることも可能である。この場合には、上記で示した手順で、設定済みカットスルーパス数>=保持される次段情報数の条件は、マージ対象となるカットスルーパスが既に設定されている、という条件になり、設定済みカットスルーパス数<保持される次段情報数の条件は、マージ対象となるカットスルーパスが未だ設定されていない、という条件になる(なお、図4の手順においては、この条件も使用できる)。

【0098】次に、選択可能な複数の次段情報に対応する各ネットワークインタフェースのリンク速度(ネットワークの帯域)が異なることを考慮する場合について説明する。

【0099】例えば、ルータ装置101のネットワークインタフェース221とネットワークインタフェース222のリンク速度が異なる場合が考えられる。従って、リンク速度を考慮して負荷分散すると好ましい。

【0100】図5に、このような場合のカットスルーパスの生成時のルータ装置101の処理手順の一例を示す。ここでは、マージしない場合について説明する。

【0101】ここでも、ルータ装置111~11Nから最終宛先をネットワーク120またはルータ装置104とするようなカットスルーパスの生成時を例にとるとともに、ネットワークインタフェース221とネットワークインタフェース222のリンク速度が1対2の場合(ネットワークインタフェース222が高速)を例にとる。

【0102】ルータ装置101のネットワークインタフェース211より受信したカットスルーパス生成用のメッセージは、ラベル処理部232においてラベルテ

ル223検索した後、自身でIP処理を行う旨を決定し、IP処理部201に転送する(ステップS501)。

【0103】設定メッセージを転送されたIP処理部201では、自身が受信すべきメッセージがどうかの判断を行い、カットスループロトコル用のメッセージの場合には、カットスルー制御部202にデータが送られる(ステップS502)。

【0104】一方、IP処理部201にて自身で受信すべきメッセージでないと判断した場合には、IP等のデータグラム転送処理を行うが、このときに、IP処理部201は、ルーチングテーブル203を検索した後、次のルータ装置を決定し、次のルータ装置にデータを転送する(ステップS503)。なお、このとき、ルータ装置101にてIP転送機能を有さない場合には、データを廃棄しても構わない。

【0105】さて、IP処理部201より設定メッセージを受信したカットスルー制御部202では、メッセージに含まれる情報より、カットスルーパスを生成するための最終宛先を獲得する(ステップS504)。

【0106】メッセージより獲得した最終宛先からルーチングテーブル203を検索して、次段のルータ装置を求める(ステップS505)。最終宛先が到達不能の場合には、そのメッセージの転送は停止される(ステップS506)。

【0107】なお、メッセージの転送が停止された後の動作は、カットスルー生成プロトコルによって異なり、ルータ装置101から前段のルータ装置111~11Nに対し、応答を返すものや、そのままプロトコル動作を停止しておくものが存在する。

【0108】一方、ステップS505にて最終宛先が存在する場合には、そのルーチングテーブル203のエントリより次段のルータ装置の情報を獲得可能であり、図1のルータ装置101の場合には、既に述べたようにルータ装置104およびネットワーク120に対してはルータ装置102およびルータ装置103が次段情報として保持されている。

【0109】カットスルー制御部202では、次段ルータ装置を選択することになるが、このときに、同一最終宛先に対し、既に設定されているカットスルーパスの本数を確認する(ステップS507)。

【0110】設定済みカットスルー数は、次段情報を求めるための判断に使用し、例えば、設定済みカットスルー数が3の倍数の場合にはルータ装置102を選択し、それ以外の場合には、ルータ装置103を選択するようなアルゴリズムにより、次段情報が決定される(ステップS508)。

【0111】なお、次段情報がn存在し、各次段iに対するリンク速度が $r(i)$ である場合には、設定済みカットスルー数をcとすると、例えば、 $y = c \bmod$

10

20

30

40

50

($r(1) + \dots + r(n)$) の値に基づいて、各次段ルータ装置をリンク速度に応じた頻度で選択していけばよい(次段 i を選択すべき y の値の個数(種類数)を、次段 i のリンク速度 $r(i)$ に比例させる)。

【0112】例えば、次段情報が3つ存在し(次段1、次段2、次段3とする)、次段1に対するリンク速度:次段2に対するリンク速度:次段3に対するリンク速度 = 1:2:3である場合(リンク速度の比の要素(この場合、1、2、3)の総和=6)、 $y = c \bmod$ リンク速度の比の要素の総和(=6)の値が0ならば次段3を選択し、1、2、3、4、5ならば、それぞれ、次段2、次段1、次段3、次段2、次段3を選択する、というような方法を用いてもよい。

【0113】また、選択のアルゴリズムについては上記のものに制限されるものではなく、各次段ルータ装置へのパス数の比率がリンク速度の比率と一致(もしくはほぼ一致)させることができるような方法であれば、どのようなものでも良い。

【0114】このようにして次段ルータを決定したカットスルー制御部202では、次段ルータに対し設定メッセージが、次段ルータがルータ装置102の場合にはネットワークインタフェース221を通じ、ルータ装置103の場合にはネットワークインタフェース222を通じて、送出される(ステップS509)。

【0115】この後、カットスルーの終点であるルータ装置104もしくは途中のルータからの設定完了のメッセージが到着することで(ステップS510)、受信したメッセージ中に含まれるフロー情報とラベル情報とそれに対応する送信フロー情報とラベル情報の関連付けが完了し、入力インタフェース上211~211N上から出力インタフェース221または222へのカットスルーパスの設定が可能となり、カットスルー転送への移行が可能となる(ステップS511)。

【0116】カットスルー転送への移行は、図2のような構成のルータ装置の場合には、受信インタフェース211~211N上に存在するラベルスイッチテーブル上に、出力ラベル情報を設定することで完了となる。

【0117】このように、基本的にリンク速度が異なる場合には、次段ルータ装置の選択のアルゴリズムを変更するだけで対応可能であることがわかる。

【0118】なお、リンク速度の相違を考慮する場合で、かつ、マージされるスイッチを使用する(マージを行う)場合についても、図4の例について行った説明とほとんど同様であり、ただステップS408の選択処理を例えば図5のステップS508のようにリンク速度を考慮したものに変更すればよい。

【0119】また、本実施形態では、図3~図5の処理にて次段情報の決定時、すなわち、ステップS308、ステップS408、ステップS508の処理アルゴリズムを変更することで、マージする場合についても、マ

ジしない場合についても、様々な用途およびロードバランスを実施することが可能である。そのいくつかの応用例を以下に示す。

【0120】ルータ装置101では、ルータ装置104またはネットワーク120以外にも、様々なカットスルーパスが生成されることがある。例えば、ルータ装置101では、別の宛先へのカットスルーパスについて、ルータ装置102を次段ルータ装置として既に設定されたカットスルーパスの数とルータ装置103を次段ルータ装置として既に設定されたカットスルーパスの数を考慮し、どちらか一方(例えば、ルータ装置102とする)が多く設定されている場合には、他方のルータ装置(この場合、ルータ装置103)への選択確率が上がるように、重み付けする。これにより、ルータ装置102およびルータ装置103に対するトータルのカットスルーパスのバランスを取ることが可能である。

【0121】また、カットスルーパスの生成時にエッジルータ装置にて、QoS情報が含まれているような場合には、既にQoSを含んで設定されているカットスルーパス数によって、指定QoSを満足していることが容易なルータ装置を選択するように、アルゴリズムを変更すればよい。

【0122】その他にも、種々のバリエーションが考えられる。

【0123】次に、図6に、本実施形態におけるIP等のヘッダ情報から次段情報を求めるために使用するルーチングテーブル203の構成例を示す。

【0124】宛先アドレス601の欄は、転送時および設定メッセージの宛先アドレス情報から次段情報を求めるためのキーとなる情報である。

【0125】次段情報602の欄は、該当する宛先情報について保持する次段情報の数を保持するために使用し、マルチパスの場合には2以上の値が設定されている。

【0126】次段情報611~61Nは、該当する宛先情報ヘッダグラムを転送するための次段情報のアドレスを保持するもので、次段情報602で設定された値によって、エントリ数に変化する。ただし、このエントリには、実際の次段ルータ装置のアドレス情報が入っている必要はなく、次段ルータ装置情報が格納されている情報の位置を示すような情報でも構わない。

【0127】カットスルー設定数603の欄は、該当する宛先情報について、既に設定されているカットスルーパスの設定数を表し、図3~図5等で示した処理について、複数存在する次段ルータ装置を決定する処理で使用する場合がある。

【0128】図7に、本実施形態における受信したデータグラム(フレーム)に付加されるラベル値から送出インタフェースや送出ラベルを求め、IP処理を介さずに転送するために使用するラベルスイッチテーブル233

の構成例を示す。

【0129】受信ラベル701の欄は、受信フレームのヘッダ情報に含まれるラベルと一致するもので、本テーブルの検索のキーとなるものである。ATMの場合にはVPI/VC Iが使用される。

【0130】送信インタフェース702は、送出すべきネットワークインタフェースを指定するもので、スイッチ部204にてスイッチするために使用する。

【0131】送出ラベル値欄703は、次のルータ装置に送るために付加するラベル、および物理レイヤが異なる場合にはその物理レイヤに関するヘッダ情報を格納するために使用される。

【0132】以上のように本実施形態によれば、ロードバランスを実行する場合に、エッジルータの関与なしに、実際にマルチパス情報を持つルータ装置のみに行うことができる。

【0133】また、制御や実装の複雑化を回避し、効果的なロードバランスを実現することができる。

【0134】さて、これまでは、カットスルーパスの設定、特に負荷分散のための次段の選択について説明してきたが、以下では、実際に流れるトラフィック量に応じて行うカットスルーパスの再設定について説明する。

【0135】図8に、実際に流れるトラフィック量に応じてカットスルーパスの再設定を行う機能を持たせたルータ装置101の構成例を示す。

【0136】IP処理部801は、IPデータグラムの宛先情報に基づいて当該データグラムが自分宛のものである否か調べ、自分宛のデータグラムについては、受信処理を行って、上位のプロトコル（例えば、TCP）に転送し、自分宛でないものについては、次の転送先を決定し、次段のルータ装置に転送するための処理を行う。

【0137】なお、ルータ装置101では、ラベルによるスイッチング機能を有するため、後者の自分宛でないデータグラムに対する転送機能を有する必要性は必ずしもない。

【0138】カットスルー制御部802は、隣接するルータ装置との間でデータグラムフローおよびラベル情報について共通の認識を得る（データグラムフローとラベルの情報をやり取りする）ために使用するプロトコルを実行する部分である。

【0139】ルーティングテーブル803は、宛先アドレスから次に送るべきルータ装置を求めるためのテーブルであり、次段情報は複数持つことも可能であるが、経路によってはマルチパスが存在しない場合もあるので、必ずしも複数ではない。

【0140】ネットワークインタフェース811～81Nは、それぞれルータ装置111～11Nと接続されるもので、物理層としては、FANP、TDP、LDP等が使用可能なものであれば何でも良く、例えばATM、フレームリレー、イーサネットなどが考えられる。

【0141】ネットワークインタフェース821は、ルータ装置102に接続され、動作としてはネットワークインタフェース811～81Nと同様のものである（ここでは、ネットワークインタフェース811～81Nと同一構成とする）。

【0142】ネットワークインタフェース822は、ルータ装置103に接続され、動作としてはネットワークインタフェース811～81Nと同様のものである（ここでは、ネットワークインタフェース811～81Nと同一構成とする）。

【0143】スイッチ部804は、カットスルー転送が可能な場合には、ネットワークインタフェースからネットワークインタフェースへと直接スイッチング可能となるようなスイッチ装置である。

【0144】各ネットワークインタフェースの構成について、ネットワークインタフェース821を例に取って説明する。

【0145】物理層処理部831は、ネットワークインタフェースが収容する物理層に応じて異なる処理が行われるが、ATMの場合にはセル同期等の処理、イーサネットの場合にはMAC処理等が、物理層処理にあたる。

【0146】物理層カウンタ832は、ネットワークインタフェース821から送出される物理層フレーム数を保持するものである。

【0147】ラベル処理部833は、受信したデータグラム（フレーム）のヘッダ情報よりラベルを抽出した後、ラベルテーブル833を検索することで、次のルータ装置へのラベルを決定し、IP処理を実行せずに、ラベルスイッチ部804を通じてそのまま次のルータに転送するための処理を行うものである。

【0148】なお、ATMの場合には、ラベル処理部833およびラベルテーブル834は、ATMスイッチ等で使用するVPI/VC Iによるスイッチテーブルがそのまま使用可能であり、ルータ装置101が全てATMの場合には、ネットワークインタフェース811～81N、821、822、ラベル処理部832、ラベルテーブル833、スイッチ部804の全ての機能がATMスイッチで実現可能となる。

【0149】実際に流れるトラフィック量に応じたカットスルーパスの再設定手順としては、概略的には、対象となるネットワークインタフェース毎にトラフィック量の計数値を定期的に参照し、所定の基準に従ってカットスルーパスを再設定すべきか否かを判断し、再設定すべきと判断された場合に、所定の方法で選択した1または複数のカットスルーパスの再設定（マージが行われていない場合には設定/解放、マージが行われている場合にはラベルスイッチテーブルの内容変更）を逐次的にもしくは纏めて行う。

【0150】図9に、図1に示したネットワークにおいて、例えばルータ装置111～11Nが最終宛先をネッ

ネットワーク120またはルータ装置104とするカットスルーを、図3に例示した方法等で生成した後に、実際の送出トラヒックを測定し、カットスルーパスの再設定を行う処理手順の一例を示す。ここでは、ルータ装置101でマージしない場合の例について示す。

【0151】この手順は、適当なタイミングで、繰り返し実行するものとする。

【0152】ルータ装置101では、ルーチングテーブル803でマルチパスが存在する場合（本例では、ネットワーク120およびルータ装置104）に、その出力インタフェースとして、指定されたものについて、トラヒックを測定する（ステップS901）。この場合、測定されるのはネットワークインタフェース821とネットワークインタフェース822である。

【0153】トラヒックの測定は設定したカットスルーパス上のトラヒックでも可能であるが、バランスが取れているかどうかの確認のためには、ネットワークインタフェース821上に存在する物理層カウンタ832を用いた方が効率は良い。ネットワークインタフェース822についても同様である。

【0154】ネットワークインタフェース821とネットワークインタフェース822についてそれぞれの物理層カウンタ832により送出カウンタ値を取得したならば、両者の送出カウンタ値を比較あるいは評価して、それら値の関係（例えば、比率）が許容範囲であるかどうかをチェックする（ステップS902）。

【0155】ここで、許容範囲とは、ネットワークインタフェース821とネットワークインタフェース822のリンク速度や使用率によって決定されるもので、例えばネットワークインタフェース821のトラフィック量の計数値とネットワークインタフェース822のトラフィック量の計数値との比がそれらのリンク速度の比率に一致もしくは近似していることが好ましい。また、双方ともトラヒックが少ない場合にはバランスがとれていなくても許容範囲としても良い。

【0156】上記のチェック後、許容範囲内の場合には、トラヒック的にはバランスが取れているものとして終了して良い（ステップS903）。

【0157】一方、ステップS902において許容範囲を超えている場合には、送出量の多いネットワークインタフェース（例えばネットワークインタフェース821側とする）において、マルチパスで設定されたカットスルーパスの中から再設定対象とするカットスルーパスを1つ選択し（ステップS904）、該選択したカットスルーパスを流れるトラヒック量の計数値を調べる（ステップS905）。

【0158】次に、チェックしたカットスルーパスのトラヒック量 x を送出量の少ないネットワークインタフェース（822）のトラヒック量 M に加算した値（ $M+x$ ）と、該チェックしたカットスルーパスのトラヒック

量 x を送出量の多いネットワークインタフェースフェース（821）のトラヒック量 N から減算した値（ $N-x$ ）とを比較もしくは評価して（ステップS906）、許容範囲、送出量の多いネットワークインタフェース（821）側に偏り過ぎ、送出量の少ないネットワークインタフェース（822）側に偏り過ぎをチェックする。

【0159】許容範囲または送出量の多いネットワークインタフェース（821）側に偏っている場合には、トラヒックを測定したカットスルーパスの次段ルータを、送出量の多いネットワークインタフェース（821）に対応するルータ装置（102）から送出量の少ないネットワークインタフェース（822）に対応するルータ装置（103）に切り替えるようにカットスルーパスの再設定を行い（ステップS907）、そして、許容範囲の場合は終了となり（ステップS908）、送出量の多いネットワークインタフェース（821）に偏っている場合には、ステップS904以降の処理を繰り返す（ステップS909）。

【0160】再設定方法は、カットスループロトコルによって異なり、カットスルーパスを解放後に設定するものと、設定後に解放処理を行うものがある。

【0161】一方、送出量の少ないネットワークインタフェース（822）側に偏っている場合には、測定したカットスルーパスの出力先を変更せずに、別のカットスルーパスを切り替えるために、ステップS904以降の処理を繰り返す（ステップS910）。

【0162】このような方法の場合には、バランスが許容範囲に達しない場合も考えられるが、その場合には、現状の状態と再設定後に想定される状態とで、許容範囲に近い方法を取ることも考えられる。

【0163】次に、図10に、図1に示したネットワークにおいて、例えばルータ装置111～11Nが最終宛先をネットワーク120またはルータ装置104とするカットスルーを、図4に例示した方法等で生成した後に、実際の送出トラヒックを測定し、カットスルーパスの再設定を行う処理手順の一例を示す。ここでは、ルータ装置101でマージする場合の例について示す。

【0164】この手順は、適当なタイミングで、繰り返し実行するものとする。

【0165】ルータ装置101では、ルーチングテーブル803でマルチパスが存在する場合（本例では、ネットワーク120およびルータ装置104）に、その出力インタフェースとして、指定されたものについて、トラヒックを測定する（ステップS1001）。この場合、測定されるのはネットワークインタフェース821とネットワークインタフェース822である。

【0166】トラヒックの測定は設定したカットスルーパス上のトラヒックでも可能であるが、バランスが取れているかどうかの確認のためには、ネットワークインタ

フェース821上に存在する物理層カウンタ832を用いた方が効率は良い。ネットワークインタフェース822についても同様である。

【0167】ネットワークインタフェース821とネットワークインタフェース822についてそれぞれの物理層カウンタ832により送出カウンタを取得したならば、両者の送出カウンタを比較あるいは評価して、それら値の関係（例えば、比率）が許容範囲であるかどうかをチェックする（ステップS1002）。

【0168】ここで、許容範囲とは、ネットワークインタフェース821とネットワークインタフェース822のリンク速度や使用率によって決定されるもので、例えばネットワークインタフェース821のトラフィック量の計数値とネットワークインタフェース822のトラフィック量の計数値との比がそれらのリンク速度の比率に一致もしくは近似していることが好ましい。また、双方ともトラフィックが少ない場合にはバランスがとれていなくても許容範囲としても良い。

【0169】上記のチェック後、許容範囲内の場合には、トラヒック的にはバランスが取れているものとして終了して良い（ステップS1003）。

【0170】一方、ステップS1002において許容範囲を超えている場合には、送出量の多いネットワークインタフェース（例えばネットワークインタフェース821側とする）において、マルチパスで設定されたカットスルーパスの中から再設定対象とするカットスルーパスを1つ選択し（ステップS1004）、該選択したカットスルーパスを流れるトラフィック量の計数値を調べる（ステップS1005）。

【0171】ここで、注意すべき点は、各カットスルーパスの送出トラヒックは既にマージされた後であるため、マージする前の受信トラヒックを測定する必要がある。

【0172】次に、チェックしたカットスルーパスのトラフィック量 x を送出量の少ないネットワークインタフェース（822）のトラフィック量 M に加算した値 $(M+x)$ と、該チェックしたカットスルーパスのトラフィック量 x を送出量の多いネットワークインタフェースフェース（821）のトラフィック量 N から減算した値 $(N-x)$ とを比較もしくは評価して（ステップS1006）、許容範囲、ネットワークインタフェース821側に偏り過ぎ、ネットワークインタフェース822側に偏り過ぎをチェックする。

【0173】許容範囲または送出量の多いネットワークインタフェースフェース（821）側に偏っている場合には、トラヒックを測定したカットスルーパスのラベルスイッチテーブル823を、送出量の少ないネットワークインタフェース（822）に出力するラベルに書き換える（ステップS1007）。そして、設定後、ステップS1006の処理で許容範囲になっている場合は終了

となり（ステップS1008）、送出量の多いネットワークインタフェースフェース（821）に偏っている場合には、ステップS1004以降の処理を繰り返す（ステップS1009）。

【0174】ここで、出力先を変更したカットスルーパスについて、プロトコル処理が必要か否かは、使用しているプロトコルに依存する。

【0175】一方、送出量の少ないネットワークインタフェース（822）側に偏っている場合には、測定したカットスルーパスの出力先を変更せずに、別のカットスルーパスを切り替えるためにステップS1004以降の処理を繰り返す（ステップS1010）。

【0176】このような方法の場合には、バランスが許容範囲に達しない場合も考えられるが、その場合には、現状の状態と再設定後に想定される状態とで、許容範囲に近い方法を取ることも考えられる。

【0177】なお、図9の手順のステップS906や図10の手順のステップS1006における比較あるいは評価の基準としては、種々のものが考えられる。

【0178】例えば、選択したカットスルーパスを再設定すると、トラフィック量の大小関係が逆転するとき、すなわち $N > M$ かつ $(N-x) < (M+x)$ となるときには、選択したカットスルーパスを採用しない（再設定しない）とする場合には、 $(N-x) < (M+x)$ のとき送出量の少ないネットワークインタフェース（本例では822）側に偏り過ぎとしてステップS906／ステップS1006からステップS904／ステップS1004に戻り、それ以外で許容範囲のときステップS907／ステップS1007から終了し、それ以外のとき依然として送出量の多いネットワークインタフェース（本例では821）側に偏り過ぎとしてステップS906／ステップS1006からステップS904／ステップS1004に戻るようにしてもよい。

【0179】また、例えば、上限許容値 $\geq (N-x) / (M+x) \geq$ 下限許容値のとき許容範囲、 $(N-x) / (M+x) >$ 上限許容値のとき送出量の多いネットワークインタフェース（本例では821）側に偏り過ぎ、下限許容値 $> (N-x) / (M+x)$ のとき送出量の少ないネットワークインタフェース（本例では822）側に偏り過ぎとしてもよい。

【0180】また、図9の手順のステップS904や図10の手順のステップS1004でのカットスルーパスの選択方法としても、種々のものが考えられる。

【0181】例えば、ラベルスイッチテーブル834のエントリを1つずつ整列順に選択していてもよい。また、例えば、ラベルスイッチテーブル834のエントリをそのトラフィック量の計数値の多いものから順に選択していてもよい。

【0182】また、図9や図10の手順例では、再設定対象とする1つのカットスルーパスの選択／選択したカ

ットスループスを再設定するか否かの判断／再設定すると判断された場合の再設定／繰り返し処理を続行するか否かの判断といった一連の処理を繰り返し行うものであったが、最初に再設定対象とするカットスループスの選択を行い、後でまとめて再設定を行うようにしてもよい。

【0183】また、各ネットワークインタフェースのトラフィック量と、マルチパスで設定された各カットスループスのトラフィック量とを考慮して、再設定すべき1または複数のカットスループスの最適な解もしくは次善の解を求めるようにしてもよい。この場合に、解が複数ある場合には、再設定すべきカットスループスの数が最小ものを選択するようにしてもよい。また、解が複数ある場合に、得られるバランスの程度や再設定すべきカットスループスの数などを総合的に勘案して解を選択するようにしてもよい。

【0184】次に、図11に、本実施形態における受信したデータグラム（フレーム）に付加されるラベル値から送出インタフェースや送出ラベルを求め、IP処理を介さずに転送するために使用するラベルスイッチテーブル834の構成例を示す。

【0185】受信ラベル1101の欄は、受信フレームのヘッダ情報に含まれるラベルと一致するもので、本テーブルの検索のキーとなるものである。ATMの場合にはVPI／VCIが使用される。

【0186】送信インタフェース1102は、送出すべきネットワークインタフェースを指定するもので、スイッチ部804にてスイッチするために使用する。

【0187】送出ラベル値欄1103は、次のルータ装置に送るために付加するラベルおよび物理レイヤが異なる場合には、その物理レイヤに関するヘッダ情報を格納するために使用される。

【0188】受信フレーム数欄1104は、このラベルテーブル情報によって転送されたフレーム数を意味し、図9や図10で示したカットスループス単位のトラフィック測定時に参照される。

【0189】本実施形態によれば、実際に流れるトラフィック量に応じてカットスループスの再設定を行うので、より効果的なロードバランスを実現することができる。

【0190】図1～図7で説明したルータ装置や設定手順に係る発明と、図1、8～11で説明したルータ装置や再設定手順に係る発明は、組み合わせで実施することも可能であるし、独立して実施することも可能である。

【0191】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0192】また、各発明の各実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータに所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体として

も実施することもできる。

【0193】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0194】さて、以下では、図12～図20を参照しながら、他の発明の実施の形態等について説明する。

【0195】本発明は、例えば、一つ以上のVPNを収容するルータ装置（ラベルスイッチルータ装置）、その通信方法などに関するものである。

10 【0196】（従来の技術）ラベルスイッチの機能を有するルータから成る非プライベートネットワーク上で動作するVPN（Virtual Private Network；仮想的プライベートネットワーク）を構築することに関心が集まっている。そこでは、プライベートネットワークの各拠点が互いに離れている場合において、各拠点のCPE（Customer Premise Equipment）を非プライベートネットワーク上のLSP（Label Switched Path；ラベルスイッチパス）で相互接続する。設定された各LSP上には、VPNに属するパケットのみが流れ、
20 そうでないパケットは流れない。

【0197】非プライベートネットワーク上の端に在って、上記LSPを終端し、かつ、特定のプライベートネットワーク拠点を、そのCPEと接続することによって収容する装置をエッジルータと呼ぶ。複数の互いに異なるVPNが非プライベートネットワーク上に構築される場合もある。その中で一つのエッジルータが互いに異なるアドレス空間に属する複数のプライベートネットワークを収容する場合もある。

30 【0198】エッジルータは、非プライベートネットワーク側のインタフェースを備え、かつ、収容する各々のCPEと接続する各々のプライベートネットワーク側のインタフェースを備える。

【0199】この種のエッジルータの従来型としては、二種類のネットワーク層処理モジュール、すなわち、非プライベート側のモジュールとプライベート側のモジュールから構成されるものが知られている。

【0200】非プライベート側のモジュールとプライベート側のモジュールの両者は互いにネットワークインタフェースで相互接続される。両者はLDP（Label Distribution Protocol）を実行することで両者間のLSPを形成する。一方、非プライベート側のLSPは、上記両者間のLSPとは互いに独立しているが、これらをスイッチングにて直接接続することで、最終的にLSPの終端インタフェースをプライベート側のモジュールに延長するようにしている。
40

【0201】このようなLSP終端インタフェースは、バーチャルネットワークインタフェースと呼ばれる。なお、一つのエッジルータ装置が複数のVPNを収容する場合は、それ相応数のプライベート側モジュールを備え
50

る。

【0202】このようなエッジルータ装置は、非プライベート側のモジュールとプライベート側モジュールとが分離された個別の装置としてもよいが、その場合、非プライベート側の装置がエッジルータとなり、プライベート側の装置がCPEとなる。

【0203】（発明が解決しようとする課題）このような従来型装置においては、LSPをプライベート側モジュールへと伸ばす目的のために、非プライベート側のモジュールとプライベート側モジュールとが互いにLDP

で通信しなければならないため、以下のような問題がある。

【0204】ひとつは、前者もしくは後者のどちらかが、一つのモジュール上に、非プライベートアドレス空間のインタフェースとプライベートアドレス空間のインタフェースとの両方を備えなければならないことである。これは、プライベート空間を一つだけ収容する場合でさえ、モジュール上のネットワークインタフェース毎にパケットフィルタリング機能を付加しなければならず、そのためにパケット転送能力が低下するという欠点がある。

【0205】さらに、従来型装置がプライベート空間を複数収容する場合、現在一般的にネットワーク層処理の実装に使用されるソフトウェアもしくはハードウェアの技術では、パケットが属するネットワークのアドレス空間を複数識別することができないので、例えばネットワークインタフェースや経路制御テーブル等、あらゆるネットワーク構成要素にアドレス空間の識別子を付加しなければならない。すなわち、従来型装置構成では、現在の一般的なソフトウェアもしくはハードウェアに大幅な改造が必要とされ、実用化が難しいといえる。

【0206】さらなる問題は、そのような複数アドレス空間の処理機能を前提とし、プライベート側モジュールがLDPを実行しなければならないことである。これは、プライベート側モジュールの実装が複雑かつ高価になるばかりでなく、LDPの仕様が更新された場合にはその都度プライベート部の実装も更新しなければならないため、将来への適応性に欠けるといえる。

【0207】本発明は、上記のような従来型装置の欠点を除去し、プライベート側モジュールが簡易に実装でき、かつ、ラベルスイッチ標準の使用変更の際には非プライベート側のモジュールだけを変更すれば済むような、（エッジ）ルータ装置、その通信方法を提供することを目的とするものである。

【0208】（発明が解決しようとする課題）本発明（請求項15）は、プライベートアドレス空間から成るプライベートネットワークに接続されパケットを転送する手段を有するプライベート処理モジュールと、非プライベートアドレス空間から成る非プライベートネットワークに接続されパケットをラベルスイッチする手段を有

する非プライベート処理モジュールと、を備えるシステム（エッジルータ装置、もしくは、エッジルータとCPEから成るシステム）における通信方法であって、前記非プライベート処理モジュールは、前記プライベート処理モジュールが接続されたプライベートネットワークと前記プライベートアドレス空間を共有する他のプライベートネットワークを収容する他のシステムが前記プライベートネットワークに存在することを認識した場合に、当該他のシステムへ向けて前記非プライベートネットワークを経由するラベルスイッチパスを設定するためのプロトコル通信を行い、前記非プライベート処理モジュールは、設定された前記ラベルスイッチパスを前記プライベート処理モジュールまで延長し、前記プライベート処理モジュールに前記他のシステムのプライベートアドレスを通知し（前記プライベート処理モジュール内に前記他のシステムに対応するバーチャルインタフェースを生成し）、前記プライベート処理モジュールは、前記他のシステムのプライベートアドレス宛のパケットを、延長された前記ラベルスイッチパスへ転送することを特徴とする。

【0209】これにより、プライベート処理モジュールがラベルスイッチパスを設定するためのプロトコル通信を行わなくとも、また、非プライベート処理モジュールが各VPN（Virtual Private Network）のプライベートアドレス空間を管理しなくとも、プライベート処理モジュールを端点とするラベルスイッチパスを設定することができ、同一VPNに属するプライベートネットワーク同士を非プライベート（公衆）ネットワークを介してラベルスイッチパスで結ぶことが簡易に実現できる。

【0210】好ましくは、前記プライベート処理モジュールと前記非プライベート処理モジュールとの間に予め複数のパス（例えば仮想コネクション）を用意しておき、前記ラベルスイッチパスの延長は、この複数のパスから選択した一つのパスと、設定された前記ラベルスイッチングパスとを、前記非プライベート処理モジュール内で対応付けることにより行い、前記他のシステムのプライベートアドレスは、選択された前記一つのパスと対応付けて通知されるようにしてもよい。

【0211】好ましくは、前記ラベルスイッチパスの延長は、前記ラベルスイッチパスが前記他のシステムに到達するように設定されたことが確認された後に行うようにしてもよい。

【0212】非プライベート処理モジュールがラベルスイッチパスを延長し、相手方のシステムに対応するバーチャルインタフェースをプライベート処理モジュール内に生成するタイミングは、少なくとも自システムの隣接ノードまでラベルスイッチパスが設定された後であっても良いが、これだと非プライベートネットワークの内部でラベルスイッチパスが終端してしまっている場合に、

自システムのプライベート処理モジュールから転送されたパケットが行き先不明により失われてしまう可能性がある。上記のように、このタイミングを、相手方のシステムまで到達するようにラベルスイッチパスが設定された後とすれば、このようなパケットロスを防ぐことができる。

【0213】好ましくは、前記他のシステムのプライベートアドレスの通知は、パケットを前記他のシステムへ運ぶための前記ラベルスイッチと、パケットを前記他のシステムから運ぶための別のラベルスイッチとの双方が設定された場合に行うようにしてもよい。

【0214】このようにすると、二つのラベルスイッチを組にして相手方のシステムと双方向通信ができる状態になったときに、相手方のシステムに対応する一つのバーチャルインタフェースがプライベート処理モジュール内に生成されることになり、プライベート処理モジュールは本発明でのバーチャルインターフェースを通常のネットワークインタフェースと同様に扱うことが可能になる。

【0215】好ましくは、前記システムは、前記プライベートアドレス空間とは異なるプライベートアドレス空間から成る第二のプライベートネットワークに接続されパケットを転送する手段を有する第二のプライベート処理モジュールをも備えるものであり、前記非プライベート処理モジュールは、前記第二のプライベート処理モジュールが接続された第二のプライベートネットワークと前記異なるプライベートアドレス空間を共有する他の第二のプライベートネットワークを収容する他のシステムが前記非プライベートネットワークに存在することを認識した場合にも、当該他のシステムへ向けて前記非プライベートネットワークを経由するラベルスイッチパスを設定するためのプロトコル通信を行い、前記非プライベート処理モジュールは、設定された前記ラベルスイッチパスを前記第二のプライベート処理モジュールまで延長し、前記第二のプライベート処理モジュールに前記他のシステムのプライベートアドレスを通知し、前記第二のプライベート処理モジュールは、前記他のシステムのプライベートアドレス宛のパケットを、延長された前記ラベルスイッチパスへ転送するようにしてもよい。

【0216】このように、本発明によれば、複数のプライベートアドレス空間を一つのエッジシステムで収容する場合に、新たに収容するプライベートアドレス空間に対応して、プライベートアドレス空間が一つである場合と同様な構成のプライベート処理モジュールをもう一つ新たに非プライベート処理モジュールにつなげるだけで良いため、拡張性の高いエッジシステムを実現できる。

【0217】ここで、もう少し本発明の作用効果に関連して説明すると、本発明によれば、例えば、エッジルータ装置等において、その非プライベート処理モジュールとプライベート処理モジュールとの間ではLSP設定プ

ロトコルを実行する必要が無く、各々のネットワークモジュールが単一のネットワーク空間のみを処理すればよいことになる。非プライベート処理モジュールは、非プライベートネットワーク空間に属するネットワーク層の処理を実行し、かつ、収容VPNのためのLSPを設定するプロトコルを実行する。一方、プライベート処理モジュールは、プライベートアドレス空間に属するネットワーク層の処理を実行する。

【0218】非プライベートネットワーク上で形成されたLSPは、一旦、非プライベート処理モジュールで終端するが、例えば、両モジュール同士を内部的に接続するパスと前記LSPとを、スイッチ部の操作などによって、実質的なLSPの端点をプライベート処理モジュールに延長する。そのとき、プライベート処理モジュールは、その端点をバーチャルネットワークインタフェースとして扱うが、そのために必要な情報は、非プライベート処理モジュール（内の例えばLSP設定プロトコル制御部）から得られ、例えば、それを、任意の下位レイヤプロトコルの拡張により、非プライベート処理モジュールがプライベート処理モジュールに対して通知するようにする。

【0219】前記下位レイヤプロトコルは、LSP設定プロトコルの仕様には依存せず、例えば、単純に、下位レイヤのパス識別情報と、LSPにて相互接続された相手方エッジルータのプライベートアドレスとのペアを与える。

【0220】以上により、プライベート処理モジュールがLSPを設定するためのプロトコル通信を行わなくとも、また、非プライベート処理モジュールが書くVPNのプライベートアドレス空間を管理しなくとも、プライベート処理モジュールを端点とするLSPを設定することができ、同一VPNに属するプライベートネットワーク同士を非プライベートネットワークを介してLSPで結ぶことが簡単に実現できる。

【0221】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0222】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0223】（発明の実施の形態）

＜実施形態2-1＞図12は、本発明におけるルータ装置を使用して、一つのVPNを収容するようなネットワーク構成の一例について示したものである。

【0224】ネットワーク1201は、VPN (Virtual Private Network) を収容す

るためのネットワークである。

【0225】ルータ装置1211~121Mは、各ルータ間にて、転送するデータグラムフローの情報と下位レイヤの情報について共通の認識を得ることで、パケットヘッダ情報を見ることなく、下位レイヤ情報だけで、高速なデータグラム転送を可能とするラベルスイッチバス（以後、LSPとも呼ぶ）を生成する機能を有する装置であり、ラベルスイッチの中段としての役割を果たすものである。

【0226】エッジルータ装置1221~122Nは、10 プライベートネットワークを収容することが可能なルータ装置であり、LSPの起点および終点となる機能を有するものである。

【0227】ネットワーク1231~123Nは、それぞれエッジルータ装置1221~122Nに収容されている。また、ネットワーク1201を介して、一つの仮想ネットワーク（以後、VPNと呼ぶ）1202を形成している。

【0228】ここで、VPNにおけるアドレス空間に関して説明しておく。

【0229】VPNを構成する各プライベートネットワークでは、そのVPN内でのみ有効なローカルなアドレス空間（以後、プライベートアドレス空間と呼ぶ）が共有して用いられる。一つのプライベートアドレス空間の中では、アドレスの重複が無い。一方、非プライベートネットワークでは、複数のVPN間で有効なアドレス空間（例えば、グローバル空間もしくはプロバイダ空間）が用いられる。

【0230】図12の例では、ネットワーク1201がグローバルアドレス空間を用いるものとし、一方、ネットワーク1231~123Nがプライベートアドレス空間を用いたVPNを構成するものとして、以後の説明を行う。

【0231】エッジルータ装置1221~122Nは、グローバルアドレス空間とプライベートアドレス空間との境界に存在しており、それぞれのアドレス空間につきそれぞれのネットワークインタフェースを備える。

【0232】図12の例では、非プライベートネットワーク1201側のネットワークインタフェース（1251~125N）にはグローバルアドレス空間に属するアドレスが付き、一方、プライベートネットワーク側のネットワークインタフェース（1261~126N）にはプライベートアドレス空間に属するアドレスが付く。以後、このプライベートアドレス空間には“1202”という識別子が与えられることとする。

【0233】ラベルスイッチバス1242~124Lは、VPN1202を構成するために、エッジルータ装置1221~122Nによって設定されたものである。

【0234】LSPを流れるデータグラムは途中のルータ装置（例えば1211~121M）ではIP処理され

ない。したがって、そのパケットヘッダにプライベートアドレスがついていても、LSPで接続されるエッジルータ装置には直接届けられる。これを利用して、各プライベートネットワーク同士が、非プライベートネットワーク上のLSPを介して、プライベートパケットをやりとりすることが可能になる。

【0235】例えば、図12のVPNでは、LSP1241~124Lの内部にはプライベートアドレス空間1202に属するパケットを流すようにする。これは、当該LSPの起点であるエッジルータ装置1221~122Nによって制御される。

【0236】図13に、図12に示したエッジルータ装置について、エッジルータ1221を例にとり、その一構成例を示す。

【0237】図13のグローバル処理モジュール1301は、非プライベートネットワークに接続するためのものである。

【0238】IP処理部1302は、ネットワーク層の処理を行うが、ここではグローバルアドレス空間に属するパケットを処理する。20

【0239】ルーティングテーブル1303は、グローバルアドレス空間に属する宛先アドレスや次段情報を管理する。

【0240】LSP制御部1304は、非プライベートネットワークを経由するラベルスイッチバスを設定するためのプロトコル（以後、LSP設定プロトコルと呼ぶ）を実行する。

【0241】ネットワークインタフェース1305は、非プライベートネットワークに接続するためのインタフェースであり、グローバルアドレス空間に属するアドレスが付き、前記LSP設定プロトコルの通信インタフェースとしても機能する。30

【0242】本ネットワークインタフェース1305の下位レイヤとしては、LSPが設定可能なものであれば、どのようなものでも良い。例えばATM、フレームリレー、イーサネットなどが考えられる。スイッチ部1306がこれを提供している。

【0243】スイッチ部1306は、データリンクにてプライベート処理モジュール1311と接続されている。40

【0244】プライベート処理モジュール1311は、プライベートネットワークを収容するためのものである。

【0245】IP処理部1312は、IP処理部1302と同様の処理を行うが、ここではプライベートアドレス空間に属するパケットを処理する。

【0246】ルーティングテーブル1313は、プライベートアドレス空間に属する宛先アドレスや次段情報を管理する。

【0247】ネットワークインタフェース1314は、50

プライベートネットワークを収容するためのインタフェースの一例であり、プライベートアドレス空間に属するアドレスが付く。

【0248】プライベート処理モジュール1311は、一つのネットワークインタフェース1314を備えているが、もし前記プライベート空間と同一空間に属するプライベートネットワークが複数あれば、それらを収容するために、同様なネットワークインタフェースを本モジュール内に相応数備えても構わない。

【0249】前記ネットワークインタフェースの下位レイヤとしては、必ずしもLSPが設定可能なものでなくても良い。一般的にネットワーク層の下で利用されている任意の下位レイヤにて実施可能である。

【0250】プライベート処理モジュール1311とグローバル処理モジュール1301とを接続するデータリンク上には、あらかじめ複数のバスを用意しておく。バスの実現例としては、該データリンクが例えばATMならば仮想コネクションにて実現できる。

【0251】各バスの識別子は、図13の例では1321~132M、1331~133Mようになる。

【0252】プライベート処理モジュール1311では、図12のようなLSPを張るためにLSP設定プロトコルを行わなくとも良いため、グローバル処理モジュール1301とは異なり、LSP制御部1304を実装しなくとも良い。

【0253】以上のように、各モジュールは、それぞれがネットワーク層の処理を行うが、一つのモジュールが複数のアドレス空間を管理しなくとも良い。

【0254】このようなネットワーク層の処理は、例えば、現在一般的なルータに使用されているソフトウェアもしくはハードウェアを組み込んで実装できる。また、そのソフトウェアもしくはハードウェアは、ネットワーク層につき一つのアドレス空間に属する処理のみを行うものでも構わない（充分である）。

【0255】図14では、各プライベートネットワークを非プライベートネットワーク上のLSPで相互接続してVPNを構築するためのエッジルータ装置の処理手順を、図12に示したエッジルータ装置1221の場合を例にとって説明する。

【0256】はじめに、エッジルータ装置1221は自分自身の初期設定を行う（ステップS1401）。

【0257】具体的には、グローバルアドレスと、プライベートアドレスならびにプライベートアドレス空間の識別子（以後、VPN識別子と呼ぶ）とをそれぞれ設定する。VPN識別子は、この例では“1202”とする。

【0258】かかる設定の際、図13の装置構成例においては、グローバル側のアドレスはグローバル処理モジュール1301のネットワークインタフェース1305に付加され、プライベート側のアドレスはプライベート

処理モジュール1311のネットワークインタフェース1314に付加される。

【0259】さらに、これらのアドレスとVPN識別子とがLSP制御部1304に記憶される。

【0260】ここで設定に使った（VPN識別子、プライベートアドレス、グローバルアドレス）の三つ組を、VPNメンバーシップ情報と呼ぶことにする。

【0261】次に、図12のエッジルータ装置1221は、LSPを設定すべき相手方のシステムの存在、すなわち、自分と同じVPN識別子“1202”を有するプライベートネットワークを収容するエッジルータ装置が自分以外にも非プライベートネットワーク1201上に存在することを認識すべく、前記VPNメンバーシップ情報を追加獲得する（ステップS1402）。

【0262】非プライベートネットワーク1201上での他者の存在を認識しなければならないため、前記メンバーシップ情報の収集は、グローバル処理モジュール1301によって実行される。かかる具体的手段としては、その際にはメンバーシップ情報を第三者によって偽られたりしないように認証等の付加的機能を持った手段が適切であるが、例えばSNMP（Simple Network Management Protocol）やLDAP（Lightweight Directory Access Protocol）等の動的な配布プロトコルや、もしくは手設定などが考えられる。

【0263】グローバル処理モジュール1301は、収集したVPNメンバーシップ情報をローカルなデータベースとして保持する。

【0264】次に、LSP制御部1304は、当該エッジルータ装置へ向けてLSPを形成するために、グローバル側のインタフェース1305からLSP設定要求メッセージを送信する（ステップS1403）。この場合は、送信用LSPの発呼を意味する。

【0265】前記LSP設定要求メッセージにおいて、フローの識別情報には、（VPN識別子、LSP起点エッジルータのグローバルアドレス、LSP終点エッジルータのグローバルアドレス）の三つ組の値を含ませるようにする。この三つ組情報を含むようなフロー識別情報を、VPNフロー識別子と呼ぶことにする。

【0266】しかる後、前記LSP設定メッセージにて要求したLSPに関するLSP設定完了通知が、図13に示したLSP処理部1304に到着すると（ステップS1404）、グローバル処理モジュール1301は、スイッチ部1306を操作し、設定された前記LSPをプライベート処理モジュール1311まで延長接続する（ステップS1405）。

【0267】例えば、エッジルータ1221からエッジルータ122Nへ到達するLSPが設定されたことを確認したときは、ラベル値136Nを持つLSPおよび識

別子の値132Mを持つバスの両者を、スイッチ部1306で接続する。

【0268】なお、この操作は、エッジルータ装置が内部的に行うことであり、非プライベートネットワーク上のLSP接続状態には影響を与えない。

【0269】ここで、前記ラベル値はLSP設定プロトコルにより割り当てられたものである。

【0270】また、前記バスの識別子は、先述のあらかじめ用意されていた複数のバスから選択した一つの識別子である。

【0271】以上の操作を行った後、グローバル処理モジュール1301は、図13に示したバーチャルインタフェース設定命令を発行し、VPN識別子に当該のプライベート処理モジュール1311内にバーチャルインタフェースを設定する(ステップS1406)。

【0272】この場合のバーチャルインタフェース設定命令では、プライベート処理モジュール1311が備えるルーティングテーブルに新たなエントリを追加記入し得る情報を通知する。

【0273】ここでは、バーチャルインタフェースの初期状態としてDOWN状態としておく。

【0274】なお、グローバル処理モジュールがLSPを延長し、相手方のエッジルータに対応するバーチャルインタフェースをプライベート処理モジュール内に設定するタイミングは、少なくとも自エッジルータの隣接ノードまでラベルスイッチバスが設定された後であっても良いが、これだと非プライベートネットワークの内部でLSPが終端してしまっている場合に、自エッジルータのプライベート処理モジュールから転送されたパケットが行き先不明により失われてしまう可能性がある。上記のように、このタイミングを、相手方のエッジルータまで到達するようにラベルスイッチバスが設定された後とすれば、このようなパケットロスを防ぐことができる。

【0275】しかる後、グローバル側のネットワークインタフェース1305にてLSP設定メッセージが到着する(ステップS1407)。

【0276】このとき、まず、エッジルータ1221はVPNメンバーシップ情報データベースを照合し、前記設定メッセージを受け付けるかどうかを判断する(ステップS1408)。

【0277】受け付けても良い場合としては、前記メッセージにてLSPのラベルに対応付けられているVPNフロー識別子について、VPN識別子と自らが収容しているプライベートネットワークのVPN識別子(この例では“1202”)とが一致し、LSP終点エッジルータのグローバルアドレスが自分自身のグローバルアドレスと一致し(以上は受信LSPの着呼を意味する)、かつ、該起点エッジルータのプライベートアドレス(これは、この時点で持っているVPNメンバーシップ情報データベースから検索できる)との間でまだ受信LSP

Pが張られていない、という条件がすべて合致するときに挙げられる。

【0278】このような場合は設定完了通知メッセージを送出し(ステップS1409)、そうでない場合は終了する(ステップS1410)。LSP設定プロトコルの仕様にも依存するが、もしNackを返す機構が定義されていれば、単に終了とせずに、Nackを返しても良い。

【0279】設定完了通知を送出したならば、図13に示したグローバル処理モジュール1301は、スイッチ部1306を操作し、設定された前記LSPをプライベート処理モジュール1311まで延長接続する(ステップS1411)。

【0280】例えば、エッジルータ122Nからエッジルータ1221へ到達するVPN1202に関するLSPの設定を受け付けたときは、ラベル値137Nを持つLSPおよび識別子の値133Mを持つバスの両者を、スイッチ部1306で接続する。

【0281】この操作の結果、LSPの実質的な終点はプライベート処理モジュール1311内のバーチャルネットワークインタフェース1341となる。

【0282】なお、この操作は、エッジルータ装置が内部的に行うことであり、非プライベートネットワーク上のLSP接続状態には影響を与えない。

【0283】また、前記ラベル値はLSP設定プロトコルにより割り当てられたものであり、前記バスの識別子は、先述のあらかじめ用意されていた複数のバスから選択した一つの識別子である。

【0284】前記LSPの延長操作を行った後、グローバル処理モジュール1301は、図13に示したバーチャルインタフェース設定命令を発行し、当該のバーチャルインタフェースをUP状態にする(ステップS1412)。

【0285】このようにすると、二つのLSPを組にして相手方のシステムと双方向通信ができる状態になったときに、相手方のシステムに対応するバーチャルインタフェースの使用が開始されることになり、プライベート処理モジュールは本発明でのバーチャルネットワークインタフェースを通常のネットワークインタフェースと同様に扱うことが可能になる。

【0286】なお、図14には省略したが、VPNメンバーシップ配布プロトコルあるいは手設定によって、自分または相手方のエッジルータが該VPNメンバーシップから脱退するという割り込みイベントが発生した時は、いかなる状態にあっても、ただちにLSPを解放し、バーチャルインタフェースそのものを消去し、初期状態へ戻る。

【0287】以上のような状態遷移は、すべて、LSP設定プロトコルを司るグローバル部モジュールもしくはメンバーシップ情報の変化によって駆動される。したが

って、図13の装置構成例においては、バーチャルインタフェースに関する制御は、すべてグローバル処理モジュール1301からの命令によって実現可能である。

【0288】また、プライベート処理モジュール1311は、それ自身がLSP設定プロトコルを実行する必要がなく、バーチャルインタフェースの制御についてはグローバル処理モジュール1301からの命令を待つだけで良いので、該プライベート空間のパケット転送や経路制御のためだけに処理能力を集中することができる。

【0289】なお、前記バーチャルインターフェース制御命令は、任意の下位レイヤプロトコルの拡張により実施可能である。

【0290】このプロトコルは、LSP設定プロトコルの仕様には依存せず、単純に、該LSPに継ぎ足されたパスの下位レイヤ情報と、LSPにて相互接続された相手方のエッジルータのプライベートアドレスとのペアとを情報として含んでいれば良い。

【0291】これまでに述べた処理手順がすべて行われると、図12に示したようにエッジルータ同士がLSPで相互接続され、お互いがプライベートアドレス空間1202での通常の通信ができるようになる。

【0292】その後は、通常のネットワークと同様の方法で経路制御プロトコルを実行することができ、各プライベートネットワーク1231～123Nの間で、プライベートアドレス空間1202に属するネットワーク通信ができるようになる。

【0293】また、これまでに述べた手順により、例えば、エッジルータ1221では、プライベート処理モジュール1311が扱うすべてのインタフェースは、プライベートアドレス空間1201に属することが保証されている。

【0294】したがって、プライベート処理モジュール1311は、バーチャルインタフェースも含め、通常のネットワークと同様の手法で、ネットワークインタフェース間のパケット転送を行うことができる。

【0295】このようなエッジルータ装置は、非プライベート処理モジュールとプライベート処理モジュールとが分離された個別の装置としても良いが、その場合、非プライベート処理モジュールがエッジルータ装置となり、プライベート処理モジュールがCPE装置となる。

【0296】なお、ここでは、双方向ともラベルスイッチパスが設定された場合にバーチャルI/Fをプライベート処理モジュール内に生成する例を示したが、どちらか一方のラベルスイッチパスしか設定されていない場合でも、そのことをプライベート処理モジュールが認識できるようにしつつバーチャルI/Fを生成するように変形実施することも可能である。

【0297】図15は、グローバル処理モジュールによって保持されるVPNメンバーシップ情報のデータベ

スの一例を示す。

【0298】例えば、図12におけるプライベートネットワーク123Nに関するVPNメンバーシップ情報を得たとすると、図15のデータベースに追加されるエントリとしては、VPN識別子の欄1501の値、プライベートアドレスの欄1502の値、グローバルアドレスの欄1503の値は、それぞれ(1202、126N、125N)となる。

【0299】図16は、LSP制御部1304によって管理される、VPNフロー識別子に関するテーブルの形式である。

【0300】VPNフロー識別子の欄1601は、そのVPN識別子が自ら収容するプライベートネットワークのVPN識別子と一致するもののみを記入するものとする。

【0301】LSPのラベル値の欄1602には、LSP設定プロトコルによって前記VPNフロー識別子に割り当てられたラベル値を記入する。

【0302】パスの識別子の欄1603には、非プライベートネットワーク上の該LSPに接続延長されたパスの識別子を記入する。

【0303】図17に、バーチャルインタフェースの構成例を示す。

【0304】図17のネットワーク層および下位レイヤの入出力1701～1704は、たとえば一般的なネットワークオペレーティングシステム実装におけるソフトウェア関数として実装しても良いし、あるいはハードウェアにて実装しても良い。

【0305】送信方向のパス1705と受信方向のパス1706とが取りまとめられ、送受信可能な一つのネットワークインタフェース1707を構成している。

【0306】このように、バーチャルネットワークインタフェースは、LSP技術に依存しない通常のネットワークインタフェースに用いられる要素だけで構成して良い。

【0307】送信方向のパスが送信用のLSPと接続されることにより、LSPの実質的な起点は本バーチャルネットワークインタフェースとなる。

【0308】受信方向のパスは、受信用のLSPと接続される。

【0309】図18に、プライベート処理モジュールが管理するルーティングテーブルの形式の一例を示す。

【0310】バーチャルインタフェース設定命令が発行された際には、宛先の欄1801には相手方エッジルータのプライベートアドレスが、次段情報の欄1802にはあらかじめ用意していた複数のパスから選択された一つのパスの識別子の値が、状態の欄1803には初期状態としてDOWN状態が、インタフェース名の欄1804にはバーチャルインタフェースの名前が、それぞれ記入される。

【0311】ただし、インタフェース名1804の値は、必ずしも前記設定命令で具体的に通知しなくとも良い。

【0312】例えば、プライベート処理モジュールが、あらかじめローカルに管理するバーチャルインタフェース名と前記バスの識別子とを対応付けておくことで、前記設定命令で通知されたバスの識別子から一意に導けば良い。

【0313】＜実施形態2-2＞図19は、本発明におけるルータ装置を使用して、複数(N個)のVPNを収容するようなネットワーク構成の一例について示したものである。

【0314】ネットワーク1901は、VPN(Virtual Private Network)を収容するためのネットワークである。

【0315】ルータ装置1911~191Mは、実施形態2-1で説明したルータ装置1211~121Mと同様の機能を有する装置である。

【0316】エッジルータ装置1920~192Nは、実施形態2-1で説明した装置1221~122Nと同様の機能を有するものである。

【0317】なお、エッジルータ装置1920のように、一つのエッジルータが複数(N個)のプライベートネットワーク1931~193Nを収容することができる点で、実施形態2-1の場合とは異なっている。

【0318】しかも、プライベートネットワーク1931~193Nは、互いに異なるVPN1941~194Nを形成している。VPNが異なれば、そのプライベートアドレス空間も互いに異なる。以後、これらアドレス空間はそれぞれ“1941”、“1942”、…、“194N”という識別子で識別されるものとする。

【0319】また、プライベートネットワーク1991~199Nは、それぞれエッジルータ装置1921~192Nに収容されているおり、それらのアドレス空間はそれぞれ“1941”、“1942”、…、“194N”という識別子で識別されるものとする。

【0320】エッジルータ装置1920~192Nは、グローバルアドレス空間とプライベートアドレス空間との境界に存在しており、それぞれのアドレス空間につきそれぞれのネットワークインタフェースを備える。

【0321】エッジルータ装置1920については、非プライベートネットワーク1901側のネットワークインタフェース1950にはグローバルアドレス空間に属するアドレスが付き、一方、プライベートネットワーク側のインタフェース1951~195Nにはそれぞれプライベートアドレス空間1941~194Nに属するアドレスが付く。

【0322】ラベルスイッチバス1961~196Nは、それぞれVPN1941~194Nを構成するために、エッジルータ装置1920~192Nによって設定

されたものである。

【0323】図20に、図19に示したエッジルータ装置について、エッジルータ装置1920を例にとり、その一構成例を示す。

【0324】本装置は、実施形態2-1で述べたものと同様の機能を有する(N+1)個のモジュールから構成される。

【0325】図20のグローバル処理モジュール2001は、非プライベートネットワークに接続するためのものである。

【0326】IP処理部2002は、ネットワーク層の処理を行うが、ここではグローバルアドレス空間に属するパケットを処理する。

【0327】ルーティングテーブル2003は、グローバルアドレス空間に属する宛先アドレスや次段情報を管理する。

【0328】LSP制御部2004は、非プライベートネットワークを経由するLSP設定プロトコルを実行する。

【0329】ネットワークインタフェース2005は、非プライベートネットワークに接続するためのインタフェースであり、グローバルアドレス空間に属するアドレスが付き、前記LSP設定プロトコルの通信インタフェースとしても機能する。

【0330】本ネットワークインタフェース2005の下位レイヤとしては、LSPが設定可能なものであれば、どのようなものでも良い。例えば、ATM、フレームリレー、イーサネットなどが考えられる。スイッチ部2006がこれを提供している。

【0331】スイッチ部2006は、データリンクにてプライベート処理モジュール2011~201Nと接続されている。

【0332】プライベート処理モジュール2011~201Nは、プライベートネットワークを収容するためのものである。

【0333】これらプライベート処理モジュールは、実施形態2-1で述べたものと同様の機能を有するが、ここでは互いに異なるプライベートアドレス空間1941~194Nに属するネットワーク層の処理を行う。

【0334】プライベート処理モジュールとグローバル処理モジュールとを接続するデータリンク上には、あらかじめ複数のバスを用意しておく。バスの実現例としては、前記データリンクが例えばATMならば仮想コネクションにて実現できる。

【0335】各バスの識別子は、図20の例では、2021~202M、2031~203Mようになる。

【0336】プライベート処理モジュール2011~201Nでは、図19のようなLSPを張るためにLSP設定プロトコルを行わなくとも良いため、グローバル部2001とは異なり、LSP制御部を実装しなくとも良

い。

【0337】非プライベートネットワーク上のLSPを利用した複数のVPNを構築するための処理手順は、図14で示した処理手順をそのまま利用することができる。

【0338】以下では、エッジルータ装置1920の場合を例にとって説明する。

【0339】はじめに、エッジルータ装置1920は、自分自身の初期設定を行う（ステップS1401）。

【0340】具体的には、グローバルアドレスと、N個のプライベートアドレスならびにプライベートアドレス空間の識別子（以後、VPN識別子と呼ぶ）とをそれぞれ設定する。VPN識別子は、この例では“1941”，“1942”，…，“194N”とする。

【0341】かかる設定の際、図20の装置構成例においては、グローバル側のアドレスはグローバル処理モジュールのネットワークインタフェース2005に付加され、N個のプライベート側のアドレスは各々のプライベート処理モジュールのネットワークインタフェースに付加される。

【0342】さらに、これらのアドレスとVPN識別子とがLSP制御部2004に記憶される。

【0343】ここで設定に使った（VPN識別子、プライベートアドレス、グローバルアドレス）の三つ組を、VPNメンバーシップ情報と呼ぶことにする。

【0344】次に、図19のエッジルータ装置1920は、LSPを設定すべき相手方のシステムの存在、すなわち、自分と同じVPN識別子1941～194Nのうちのどれかに一致するプライベートネットワークを収容するエッジルータ装置が自分以外にも非プライベートネットワーク1901上に存在することを認識すべく、前記VPNメンバーシップ情報を追加獲得する（ステップS1402）。

【0345】非プライベートネットワーク1901上での他者の存在を認識しなければならないため、前記メンバーシップ情報の収集はグローバル処理モジュール2001によって実行される。かかる具体的手段としては、実施形態2-1で述べたものと同様のものが考えられる。

【0346】グローバル処理モジュール2001内は、収集したVPNメンバーシップ情報を実施形態2-1の場合と同様なローカルなデータベースとして保持する。

【0347】次に、LSP制御部2004は、当該エッジルータ装置へ向けてLSPを形成するために、グローバル側のインタフェース2005からLSP設定要求メッセージを送信する（ステップS1403）。この場合は送信用LSPの発呼を意味する。

【0348】前記LSP設定要求メッセージにおいて、フローの識別情報には（VPN識別子、LSP起点エッジルータのグローバルアドレス、LSP終点エッジルータのグローバルアドレス）の三つ組の値を含ませるようにする。この三つ組情報を含むようなフロー識別情報を、VPNフロー識別子と呼ぶことにする。

【0349】VPNフロー識別子は、LSP制御部2004により、例えば図16に示すようなテーブルのエントリ形式にて管理される。この管理の方法は、実施形態2-1と同様である。

【0350】しかる後、前記LSP設定メッセージにて要求したLSPに関するLSP設定完了通知が、図20に示したLSP処理部2004に到着すると（ステップS1404）、グローバル処理モジュール2001は、スイッチ部2006を操作し、設定された前記LSPをプライベート処理モジュール2011まで延長接続する（ステップS1405）。

【0351】例えば、エッジルータ装置1920からエッジルータ装置192Nへ到達するLSPが設定されたことを確認したときは、ラベル値206Nを持つLSPおよび識別子の値202Mを持つバスの両者を、スイッチ部2006で接続する。

【0352】なお、この操作は、エッジルータ装置が内部的に行うことであり、非プライベートネットワーク上のLSP接続状態には影響を与えない。

【0353】ここで、前記ラベル値はLSP設定プロトコルにより割り当てられたものである。

【0354】また、前記バスの識別子は、先述のあらかじめ用意されていた複数のバスから選択した一つの識別子であり、これは図16におけるバスの識別子の欄1603に記入する。

【0355】以上の操作を行った後、グローバル処理モジュール2001は、図20に示したバーチャルインタフェース設定命令を発行し、VPN識別子に当該のプライベート処理モジュール2011内にバーチャルインタフェースを設定する（ステップS1406）。

【0356】バーチャルインタフェースの実装やバーチャルインタフェース設定命令については、実施形態2-1と同様にして実施できる。

【0357】しかる後、グローバル側のネットワークインタフェース2005にてLSP設定メッセージが到着する（ステップS1407）。

【0358】このとき、まず、エッジルータ装置1920は、VPNメンバーシップ情報データベースを照合し、前記設定メッセージを受け付けるかどうかを判断する（ステップS1408）。

【0359】受け付けても良い場合としては、前記メッセージにてLSPのラベルに対応付けられているVPNフロー識別子について、VPN識別子と自らが収容しているプライベートネットワークのVPN識別子（この例では、“1940”，“1941”，…，“194N”のどれか）とが一致し、LSP終点エッジルータのグローバルアドレスが自分自身のグローバルアドレスと一致

し（以上は受信用LSPの着呼を意味する）、かつ、該起点エッジルータのプライベートアドレス（これは、この時点で持っているVPNメンバーシップ情報データベースから検索できる）との間でまだ受信用LSPが張られていない、という条件がすべて合致するときに挙げられる。

【0360】このような場合は設定完了通知メッセージとしてAckを送出し（ステップS1409）、そうでない場合は終了する（ステップS1410）。LSP設定プロトコルの仕様にも依存するが、もしNackを返す機構が定義されていれば、単に終了とせず、Nackを返しても良い。

【0361】設定完了通知を送出したならば、図20に示したグローバル処理モジュール2001は、スイッチ部2006を操作し、設定された前記LSPを当該プライベート処理モジュールまで延長接続する（ステップS1411）。

【0362】例えば、エッジルータ装置192Nからエッジルータ装置1920へ到達するVPN194Nに関するLSPの設定を受け付けたときは、ラベル値207Nを持つLSPおよび識別子の値203Mを持つバスの両者を、スイッチ部2006で接続する。

【0363】この操作の結果、LSPの実質的な終点はプライベート処理モジュール201N内のバーチャルネットワークインタフェースとなる。

【0364】なお、この操作は、エッジルータ装置が内部的に行うことであり、非プライベートネットワーク上のLSP接続状態には影響を与えない。

【0365】また、前記ラベル値はLSP設定プロトコルにより割り当てられたものであり、前記バスの識別子は、先述のあらかじめ用意されていた複数のバスから選択した一つの識別子である。以上の情報は、図16における一つのエントリとして記入する。

【0366】前記LSPの延長操作を行った後、グローバル処理モジュール2001は、図20に示したバーチャルインタフェース設定命令を発行し、当該のバーチャルインタフェースをUP状態にする（ステップS1412）。

【0367】このようにすると、二つのLSPを組にして相手方のシステムと双方向通信ができる状態になったときに、相手方のシステムに対応するバーチャルインタフェースの使用が開始されることになり、プライベート処理モジュールは本発明でのバーチャルネットワークインタフェースを通常のネットワークインタフェースと同様に扱うことが可能になる。

【0368】なお、図14には省略したが、VPNメンバーシップ配布プロトコルあるいは手設定によって、自分または相手方のエッジルータが該VPNメンバーシップから脱退するという割り込みイベントが発生した時は、いかなる状態にあっても、ただちにLSPを解放

し、バーチャルインタフェースそのものを消去し、初期状態へ戻る。

【0369】以上のような状態遷移は、すべて、LSP設定プロトコルをつかさどるグローバル部モジュールもしくはメンバーシップ情報の変化によって駆動される。したがって、図20の装置構成例においては、バーチャルインタフェースに関する制御は、すべてグローバル処理モジュールから2001の命令によって実現可能である。

10 【0370】また、プライベート処理モジュール2011～201Nは、それ自身がLSP設定プロトコルを実行する必要がなく、バーチャルインタフェースの制御についてはグローバル処理モジュールからの命令を待っているだけで良いので、該プライベート空間のパケット転送や経路制御のためだけに処理能力を集中することができる。

【0371】なお、前記バーチャルインターフェース制御命令は、任意の下位レイヤプロトコルの拡張により実施可能である。

20 【0372】このプロトコルは、LSP設定プロトコルの仕様には依存せず、単純に、該LSPに継ぎ足されたバスの下位レイヤ情報と、LSPにて相互接続された相手方のエッジルータのプライベートアドレスとのペアとを情報として含んでいれば良い。

【0373】これまでに述べた処理手順がすべて行われると、図19に示したようにエッジルータ同士がLSPで相互接続され、お互いが固有のプライベートアドレス空間にて通常の通信ができるようになる。

30 【0374】その後は、通常のネットワークと同様の方法で経路制御プロトコルを実行することができ、プライベートネットワーク1991とプライベートネットワーク1931との間で、あるいは同様にプライベートネットワーク199Nとプライベートネットワーク193Nとの間でも、各々が固有のプライベートアドレス空間にてネットワーク通信ができるようになる。

【0375】勿論、一つのプライベートアドレス空間を共有するプライベートネットワークが複数存在する場合でも同様である。

40 【0376】また、これまで述べた手順により、例えばエッジルータ1920では、各プライベート処理モジュールが扱うすべてのインタフェースは、そのモジュール内で単一のプライベートアドレス空間に属することが保証されている。

【0377】したがって各プライベート処理モジュールは、バーチャルインタフェースも含め、通常のネットワークと同様の手法で、ネットワークインタフェース間のパケット転送を行うことができる。

50 【0378】このようなエッジルータ装置は、非プライベート処理モジュールとプライベート処理モジュールとが分離された個別の装置としても良いが、その場合、非

プライベート処理モジュールがエッジルータ装置となり、プライベート処理モジュールがCPE装置となる。

【0379】なお、ここでは、双方向ともラベルスイッチパスが設定された場合にバーチャルI/Fをプライベート処理モジュール内に生成する例を示したが、どちらか一方のラベルスイッチパスしか設定されていない場合でも、そのことをプライベート処理モジュールが認識できるようにしつつバーチャルI/Fを生成するように変形実施することも可能である。

【0380】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0381】また、各発明の各実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0382】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0383】（発明の効果）本発明によれば、各プライベート部モジュールがラベルスイッチ制御やパケットフィルタリングを行わなくとも良いので、各モジュールの実装が簡易になり、パケット転送性能を損なうことなくプライベートな通信路を実現できるので、装置あたりの性能費用比の点で有効である。また、ラベルスイッチング標準の仕様変更の際にはグローバル部モジュールのみを変更すれば済むことと、複数のプライベートアドレス空間を一つのエッジシステムで収容する場合に、新たに収容するプライベートアドレス空間に対応して、プライベートアドレス空間が一つである場合と同様な構成のプライベート処理モジュールをもう一つ新たに非プライベート処理モジュールにつなげるだけで良いことから、拡張性の高いエッジシステムを実現できる。

【0384】さて、以下では、図21～図24を参照しながら、さらに他の発明の実施の形態等について説明する。

【0385】本発明は、例えば、仮想的なプライベートネットワークを構成するためのルータ装置、その通信方法などに関するものである。

【0386】（従来の技術）VPN（Virtual Private Network；仮想的プライベートネットワーク）を実現する従来技術は、おもに二通り存在する。

【0387】一つは、プライベートなパケットを非プライベートなパケットでカプセル化する技術であり、もう一つは、プライベートなパケットを非プライベートネットワーク上のラベルスイッチパスにて転送する技術である。

【0388】前者のカプセル化技術を用いたVPNで

は、ラベルスイッチネットワークの存在を仮定せずともVPNが実現可能であるという柔軟性が利点である反面、ラベルスイッチネットワークにおけるデータ転送の高速性や通信品質の保証機能をVPN専用利用することができないという欠点があった。

【0389】一方で、後者のラベルスイッチパス技術を用いたVPNでは、ちょうど前者における利点と欠点が入れ替わることになる。

【0390】（発明が解決しようとする課題）ラベルスイッチネットワーク領域と非ラベルスイッチネットワーク領域とが混在している環境は、例えばインターネットサービスプロバイダーのバックボーンなどで、より広く一般的なものとなりつつある。

【0391】本発明は、上記のような環境のもとで、一方でラベルスイッチが利用できるネットワーク領域では自動的にVPN専用のラベルスイッチパスを設定し、他方でラベルスイッチが利用できないネットワーク領域では自動的にカプセル化を施すようなVPN実現方法を与えることで、従来の二極的なVPN技術では得られなかった柔軟かつ高速で通信品質の保証をも期待できるVPNを提供可能なルータ装置、その通信方法を提供することを目的とする。

【0392】（発明が解決しようとする課題）本発明（請求項20）は、ラベルスイッチパスをその内部に設定可能なラベルスイッチネットワークと、それ以外の非ラベルスイッチネットワークとを含み、プライベートアドレス空間を共有する少なくとも二つのプライベートネットワークの間に位置する非プライベートネットワークにおいて、仮想的なプライベートネットワークを構成するための通信方法であって、前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータが、前記プライベートネットワークの一方から当該ルータへのラベルスイッチパスを設定するのに用いられた制御メッセージの内容に基づき、該ラベルスイッチパスから受信したパケットの宛先プライベートアドレスが前記プライベートネットワークの他方であることを認識し、受信した該パケットを前記プライベートネットワークの他方に対応する非プライベートアドレスでカプセル化して送信することを特徴とする。

【0393】一方のプライベートネットワークからのラベルスイッチパスの設定に用いられる制御メッセージ中では、他方のプライベートネットワークを収容する境界ルータの非プライベートアドレスが指定され、どの仮想的なプライベートネットワーク（VPN）を構成するためのパスであるかが示されている。したがって、ラベルスイッチネットワークと非ラベルスイッチネットワークの境界にあるルータは、この制御メッセージの内容を記憶しておき、後にパケットを受信した時にこれを利用すれば、そのラベルスイッチパスから受信したパケット自体には宛先として未知のプライベートアドレスしか記入

されていなくても、そのパケットは他方のプライベートネットワークを収容する境界ルータへ送るべきであると判断でき、この判断に基づいてパケットを非プライベートアドレスでカプセル化して送信することができる。これにより、非プライベートネットワークの全体がラベルスイッチネットワークではない（一方のプライベートネットワークはラベルスイッチネットワークに接続されているが他方のプライベートネットワークは非ラベルスイッチネットワークに接続されている）環境でも、一方のプライベートネットワークからのパケットを途中まではラベルスイッチバスを利用して他方のプライベートネットワークへ転送するVPNを実現することが可能になる。

【0394】好ましくは、前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータが、前記プライベートネットワークの一方から当該ルータへのラベルスイッチバスを設定するのに用いられた制御メッセージの内容に基づき、自身が前記プライベートネットワークの境界ルータであると前記非プライベートネットワーク内に広告し、前記プライベートネットワークの他方を収容する前記非プライベートネットワークに接続されたルータは、この広告に基づいて前記プライベートネットワークの他方からのパケットを前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータの非プライベートアドレスでカプセル化して送信し、このカプセル化されたパケットを受信した前記ラベルスイッチネットワークと前記非ラベルスイッチネットワークとの境界に設置されたルータは、該カプセル化を解いて該パケットを当該ルータから前記プライベートネットワークの一方へのラベルスイッチバスへ送信するようにしてもよい。

【0395】他方のプライベートネットワークを収容する境界ルータは、一方のプライベートネットワークを収容する境界ルータとして、一方のプライベートネットワークを直接収容しラベルスイッチネットワークに接続されたルータと、ラベルスイッチネットワークと非ラベルスイッチネットワークの境界にある広告を行ったルータ（プロキシ境界ルータと解釈することもできる）とを認識するが、ネットワーク的な距離の近さから、プロキシ境界ルータの方を選択して、カプセル化送信を行う。

【0396】そして、ラベルスイッチネットワークと非ラベルスイッチネットワークの境界にあるルータは、受信したカプセル化パケットの送信元情報を調べることにより、このカプセル化パケットがどのVPNに属するプライベートネットワークを収容するどの境界ルータから送信されてきたかが分かる。この送信元情報に示される境界ルータが、一方のプライベートネットワークからラベルスイッチバスを介してパケットを受信した時にカプセル化送信の宛先とするルータであれば、そのラベルス

イッチバスとちょうど逆方向のラベルスイッチバスであって、受信したカプセル化パケットの示すVPN用のものへ、カプセル化を解いて転送すれば良いことが分かる。

【0397】このようにして、非ラベルスイッチネットワークに接続された他方のプライベートネットワークからのパケットも、途中からはラベルスイッチバスを利用してラベルスイッチネットワークに接続された一方のプライベートネットワークへ転送するVPNを実現することが可能になる。

【0398】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0399】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0400】（発明の実施の形態）図21は、ラベルスイッチネットワーク領域と非ラベルスイッチネットワーク領域との両方を含むネットワークの一例を示しており、かつ、このネットワーク上でVPNが構成されている様子を示している。

【0401】一方のネットワーク領域2101は、ラベルスイッチが利用でき、かつVPN専用のラベルスイッチバスを設定することができるような、ネットワーク1901と同様の機能を持つネットワークである。

【0402】他方のネットワーク領域2102は、前記ラベルスイッチを利用しないネットワークの一例である。

【0403】両者を併せたものが、一つの非プライベートアドレス空間（以後、グローバルアドレス空間と呼ぶ）を共有する、非プライベートネットワークであるものとする。

【0404】この非プライベートネットワークを挟んで、ネットワーク2103およびネットワーク2104が、一つのプライベートアドレス空間を共有するVPNを実現するものとする。

【0405】ルータ装置2105は、非プライベートアドレス空間のラベルスイッチネットワーク2101とプライベートアドレス空間のネットワーク2103との境界に位置し、各々の側にネットワークインタフェースを備え、ラベルスイッチバス（以下、LSPと呼ぶ）の起点および終点となる機能を有するものである。

【0406】ルータ装置2106は、非プライベートアドレス空間のラベルスイッチネットワーク2101と同一アドレス空間の非ラベルスイッチネットワーク2102との境界に位置し、各々の側にネットワークインタフェ

ースを備え、LSPの起点および終点となる機能を有し、かつ、パケットのカプセル化およびデカプセル化を行う機能を有するものである（以後、ラベルスイッチ境界ルータ装置と呼ぶ）。

【0407】ルータ装置2107は、非プライベートアドレス空間の非ラベルスイッチネットワーク2102とプライベートネットワーク2104との境界に位置し、各々の側にネットワークインタフェースを備え、パケットカプセル化およびデカプセル化を行う機能を有するものである。

【0408】LSP2108は、ルータ装置2105とルータ装置2106との間で、図14に示した処理手順と同様の処理手順にて設定された、VPNを構成するためのものである。本LSPには該VPNのプライベートアドレスが付いたパケットが流れる。

【0409】カプセル化パケット転送路2109は、同VPNを構成するためのものである。

【0410】ここでは、プライベートアドレスが付いたパケットが、非プライベートアドレスのパケットにてカプセル化されることにより、ルータ装置2106とルータ装置2107との間の非プライベートネットワーク上で、VPNのパケットが転送可能となっている。

【0411】図22に、本発明によるラベルスイッチ境界ルータ装置について、図21に示した非プライベートネットワーク上のラベルスイッチ境界ルータ装置2106を例にとり、その一構成例を示す。

【0412】IP処理部2201は、ネットワーク層の処理を行うが、ここではグローバルアドレス空間に属するパケットを処理する。

【0413】ルーティングテーブル2202は、グローバルアドレス空間に属する宛先アドレスや次段情報を管理する。

【0414】LSP制御部2203は、非プライベートネットワークを経由するLSPを設定するためのプロトコル（以後、LSP設定プロトコルと呼ぶ）を実行する。

【0415】ラベルスイッチネットワークインタフェース2204は、ラベルスイッチネットワーク2101に接続するためのネットワークインタフェースであり、グローバルアドレス空間に属するアドレスがつき、前記LSP設定プロトコルの通信インタフェースとしても機能する。

【0416】本ネットワークインタフェース2204の下位レイヤとしては、LSPが設定可能なものであれば、どのようなものでも良い。例えばATM、フレームリレー、イーサネットなどが考えられる。

【0417】ラベルスイッチネットワークインタフェースは、必要に応じて複数備えても良い。

【0418】非ラベルスイッチネットワークインタフェース2205は、非ラベルスイッチネットワーク210

2に接続するためのネットワークインタフェースであり、グローバルアドレス空間に属するアドレスがつく。

【0419】本ネットワークインタフェース2205の下位レイヤとしては、LSPが設定可能である必要はなく、一般的にネットワーク層の下で利用されている任意の下位レイヤにて実施可能である。

【0420】非ラベルスイッチネットワークインタフェースは、必要に応じて複数備えても良い。

【0421】カプセル化部2206は、特定のLSPから受信したデータグラムを、非プライベートアドレス空間のパケットヘッダでカプセル化し、非ラベルスイッチネットワークインタフェース2205に転送可能とするためのものである。

【0422】デカプセル化部2207は、非ラベルスイッチネットワークインタフェース2205にて受信した特定のデータグラムを、デカプセル化し（この場合、非プライベートアドレスが付いたパケットヘッダを除去し）、それらを特定のLSPに転送するためのものである。

【0423】図23では、ラベルスイッチネットワークと非ラベルスイッチネットワークとが混在する非プライベートネットワーク上でVPNを実現するためのラベルスイッチ境界ルータ装置の処理手順を、ラベルスイッチ境界ルータ装置2106の場合を例にとりて説明する。

【0424】ラベルスイッチ境界ルータ装置2106は、VPNメンバーシップ情報を獲得する（ステップS2301）。かかる獲得の手段は、実施形態2-1と同様のVPNメンバーシップ配布手段で実現できる。これはVPNメンバーシップ情報データベースに保持する。

【0425】図21において、例えば、ルータ装置2105に関するVPNメンバーシップ情報を得た場合、ルータ装置2105のVPN識別子とグローバルアドレスとプライベートアドレスとを認識する。また、同様にルータ装置2107に関してもVPNメンバーシップ情報を得る。

【0426】そこで、ラベルスイッチ境界ルータ装置2106は、自らも前記VPNメンバーシップに参加宣言する（ステップS2302）。

【0427】この例では、自分と同じラベルスイッチネットワークの領域に属するルータ装置2105に関して、前記情報のうち、グローバルアドレスの項を自らのグローバルアドレスにて代入したものを、ルータ装置2107に通知する。通知の手段としては先述したVPNメンバーシップ配布手段を用いることができる。

【0428】しかる後、ラベルスイッチ境界ルータ装置2106には、ラベルスイッチネットワーク2102を経由して、LSP設定メッセージが到着する（ステップS2303）。

【0429】前記LSP設定メッセージの一例として、たとえばルータ装置2105によって送出されたものを

考え、かつ、そのメッセージ中には、LSPのラベルに対応つけるVPNフロー識別子において、当該VPNの識別子ならびにLSP終点エッジルータのグローバルアドレスとしてルータ装置2107のグローバルアドレスが記入されている場合を考える。

【0430】このようなとき、ラベルスイッチ境界ルータ装置2106は、VPNメンバーシップ情報データベースを照合し前記設定メッセージを受け付けるかどうかを判断する(ステップS2304)。

【0431】VPNに関して前記設定メッセージを受け付けても良い場合の例としては、前記設定メッセージにてLSPのラベルに対応付けられているVPNフロー識別子について、VPN識別子とLSP終点エッジルータのグローバルアドレスとの組がVPNメンバーシップ情報データベースの中でマッチするエントリがあり、かつ、前記設定メッセージ中の起点エッジルータについてもVPNメンバーシップ情報データベースの中でマッチするエントリがある、という条件が合致するときに挙げられる。

【0432】設定メッセージを受け付けられない場合は、終了する(ステップS2305)。なお、LSP設定プロトコルの仕様にも依存するが、もしNackを返す機構が定義されていれば、単に終了とせずに、Nackを返しても良い。

【0433】前記設定メッセージを受け付けた場合、LSPの設定完了通知を送出する。(ステップS2306)。

【0434】この例では、LSP2108についてルータ装置2105からルータ装置2106への方向が設定完了したことに相当する。

【0435】このLSP上を流れてくるデータグラムは、パケットの宛先アドレスがプライベート空間アドレスとなっていて良い。

【0436】ラベルスイッチ境界ルータ装置2106は、前記LSPのラベルに対応付けられているVPNフロー識別子から、このLSP上を流れてくるデータグラムをデータグラムを転送すべきノードはルータ装置2107であるということを判断することができる。

【0437】この判断に基づいて、ラベルスイッチ境界ルータ装置2106は、前記LSPから受けとったデータグラムを、非プライベートアドレスのパケットヘッダにてカプセル化し、転送を開始することができる(ステップS2307)。

【0438】この例のカプセル化では、宛先アドレスはルータ装置2107のグローバルアドレスに、送信元アドレスはラベルスイッチ境界ルータ装置2106のグローバルアドレスに、それぞれ設定される。

【0439】これは、カプセル化パケット転送路2109についてルータ装置2106からルータ装置2107への方向が確立したことに相当する。

【0440】ここまでの手順で、図21において、プライベートネットワーク2103からプライベートネットワーク2104への方向に、VPNのデータグラムを到達させることが可能になる。

【0441】次に、ラベルスイッチ境界ルータ装置2106は、ルータ装置2105へ向けて、LSP設定メッセージを送出する(ステップS2308)。

【0442】この例では、先述したLSP2108の逆方向の設定を要求する。

【0443】しかる後、設定完了通知メッセージが到着すると(ステップS2309)、ラベルスイッチ境界ルータ装置2106は、ルータ装置2107から受信したカプセル化パケットをデカプセル化し、先述したルータ装置2105へ到達する当該LSPに転送を開始することができる(ステップS2310)。

【0444】例えばルータ装置2107が一つのVPNだけを収容する場合は、ラベルスイッチ境界ルータ装置2106は、カプセル化パケットの送信元アドレスとVPNメンバーシップ情報データベースとを調べることにより、そのパケットがどのVPNに属しているかを一意に定めることができ、かつ、デカプセル化してどのLSPに転送すべきかを一意に定めることができる。

【0445】ただし、ルータ装置2107から受信するパケットは必ずしもカプセル化されたパケットではないが、そのときはデカプセル化や前記特定のLSPへの転送は行わない。

【0446】また、カプセル化されたパケットであっても、もし、ルータ装置2107が複数の異なるVPNを収容している場合には、前記パケットがどのVPNに属しているかを定められるときに限り当該のLSPに転送するようにする。

【0447】カプセル化パケットがどのVPNに属しているかを定める手段としては、例えば、パケットのカプセル時に付加的情報を挿入できる手段として、GREトンネル、IPsec、L2TPなどが適用できる。図21の例では、ルータ装置2107が前記付加的情報としてVPN識別子を挿入すれば良い。

【0448】図24では、ラベルスイッチネットワークと非ラベルスイッチネットワークとが混在する非プライベートネットワーク上でVPNを実現するための、非ラベルスイッチネットワーク上のエッジルータ装置の処理手順を、図21のルータ装置2107の場合を例にとつて説明する。

【0449】カプセル化パケット転送路2109が設定されていない初期の状態において、ルータ装置2107は、先述したVPNメンバーシップ情報の収集手段を用いて、VPNメンバーシップ情報を新たに獲得する(ステップS2401)。

【0450】図21の例では、ルータ装置2105およびルータ装置2106に関する情報を認識する。

【0451】これらの情報エントリは、VPN識別子およびプライベートアドレスの項の値が同一であり、グローバルアドレスの項の値が異なっている。グローバルアドレスの項の値は、前者がルータ装置2105のグローバルアドレスであり、後者がルータ装置2106のグローバルアドレスとなっている。

【0452】そこで、ルータ装置2017は、これらルータについて比較を行い、一方のルータを選択する（ステップS2402）。かかる選択の際はさまざまな基準を用いることが可能であり、例えばルータのグローバルアドレスについてネットワーク的な距離が近い方を選択するという基準が考えられる。

【0453】ルータ装置2017は、プライベートネットワーク2104発のVPNのパケットを、非プライベートネットワーク2102を通過させるために、前記の選択したルータのグローバルアドレスにてカプセル化して、転送を開始する（ステップS2403）。

【0454】前記のルータ選択の際、ネットワークの距離的により近いルータ2106を選択したのであれば、これは、図21におけるカプセル化パケット転送路2109についてルータ装置2107からルータ装置2106への方向が確立したことに相当する。

【0455】ここまでの手順で、図21において、プライベートネットワーク2104からプライベートネットワーク2103への方向に、VPNのデータグラムを到達させることが可能になる。

【0456】以上により、プライベートネットワーク2103とプライベートネットワーク2104との間で双方向のVPNが確立する。

【0457】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0458】また、各発明の各実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0459】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0460】（発明の効果）本発明によれば、一方のプライベートネットワークはラベルスイッチネットワークに接続されているが他方のプライベートネットワークは非ラベルスイッチネットワークに接続されている環境でも、ラベルスイッチネットワーク上ではラベルスイッチパスを利用したVPNを実現することが可能になる。

【0461】

【発明の効果】本発明によれば、ロードバランスを実行する場合に、エッジルータの関与なしに、実際にマルチパス情報を持つルータ装置のみにて行うことができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るルータ装置を含むネットワークの構成例を示す図

【図2】同実施形態に係るルータ装置の構成例を示す図

【図3】カットスルーパス設定手順の一例を示すフローチャート

【図4】カットスルーパス設定手順の他の例を示すフローチャート

【図5】カットスルーパス設定手順のさらに他の例を示すフローチャート

【図6】ルーティングテーブルの一構成例を示す図

【図7】ラベルスイッチテーブルの一構成例を示す図

【図8】同実施形態に係るルータ装置の他の構成例を示す図

【図9】カットスルーパス再設定手順の一例を示すフローチャート

【図10】カットスルーパス再設定手順の他の例を示すフローチャート

【図11】ラベルスイッチテーブルの他の構成例を示す図

【図12】非プライベートネットワーク上に構築されるVPNの一例を示す図

【図13】本発明の一実施形態に係るVPNエッジルータの構成例を示す図

【図14】エッジルータの処理手順の一例を示すフローチャート

【図15】VPNメンバーシップ情報の集合から成るデータベースの一例を示す図

【図16】グローバル処理モジュールが管理するラベルに関するテーブルの一例を示す図

【図17】バーチャルインタフェースの実装例を示す図

【図18】プライベート処理モジュールにおけるルーティングテーブルの一例を示す図

【図19】非プライベートネットワーク上に構築される複数のVPNの一例を示す図

【図20】本発明の一実施形態に係るVPNエッジルータの他の構成例を示す図

【図21】ラベルスイッチ領域と非ラベルスイッチ領域とを含む非プライベートネットワーク上に実現されるVPNの一例を示す図

【図22】本発明の一実施形態に係るラベルスイッチ境界ルータ装置の構成例を示す図

【図23】ラベルスイッチ境界ルータ装置の処理手順の一例を示すフローチャート

【図24】非ラベルスイッチルータ装置の処理手順の一例を示すフローチャート

【符号の説明】

101～104, 111～11N…ルータ装置

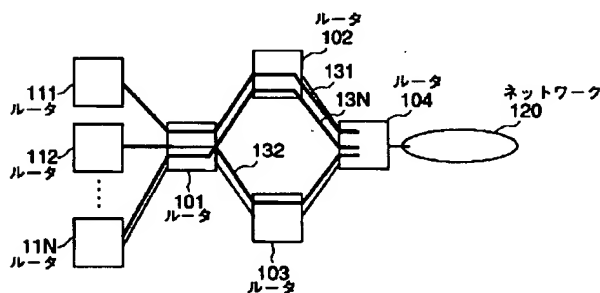
120…ネットワーク

201, 801…IP処理部

57

202, 802…カッタスルー制御部
 203, 803…ルーティングテーブル
 204, 804…スイッチ部
 211～21N, 221, 222, 811～81N, 8
 21, 822…ネットワークインタフェース
 231, 831…物理層処理部
 232, 833…ラベル処理部
 233, 834…ラベルテーブル
 832…物理カウンタ
 1221～122N, 1920～192N…エッジルー 10
 タ装置
 1211～121M, 1911～191M…ルータ装置
 1201, 1901…非プライベートネットワーク
 1231～123N, 1931～193N, 1991～
 199N…プライベートネットワーク
 1251～125N, 1261～126N, 1305,
 1314, 1950～195N, 1971～197N,
 1981～198N, 2005…ネットワークインタフ
 ェース
 1301, 2001…グローバル処理モジュール 20

【図1】

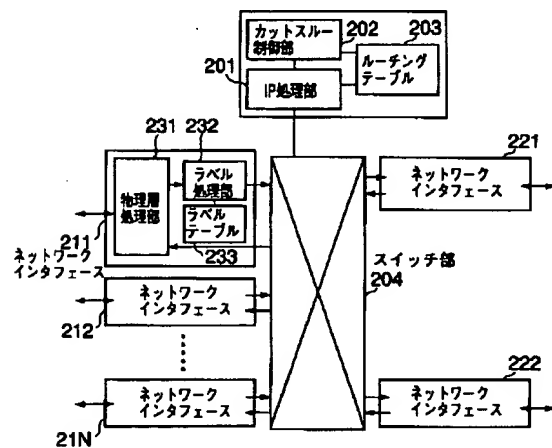


【図6】

601 宛先アドレス	602 次段情報数	611 次段情報...	61N 次段情報	603 カッタスルー 設定値
⋮	⋮	⋮	⋮	

58
 1302, 1312, 2002…IP処理部
 1303, 1313, 2003…ルーティングテーブル
 1304, 2004…LSP制御部
 1306, 2006…スイッチ部
 1311, 2011～201N…プライベート処理モジ
 ュール
 1341～134N…バーチャルインタフェース
 2101…ラベルスイッチネットワーク
 2102…非ラベルスイッチネットワーク
 2103, 2104…プライベートネットワーク
 2105～2107…ルータ装置
 2201…IP処理部
 2202…ルーティングテーブル
 2203…LSP制御部
 2204…ラベルスイッチネットワークインタフェース
 2205…非ラベルスイッチネットワークインタフェー
 ス
 2206…カプセル化部
 2207…デカプセル化部

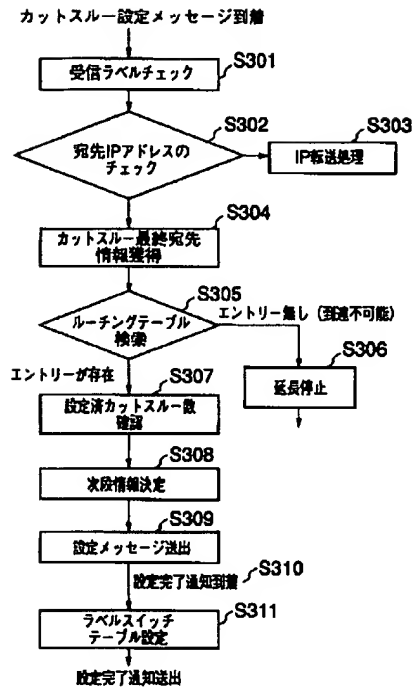
【図2】



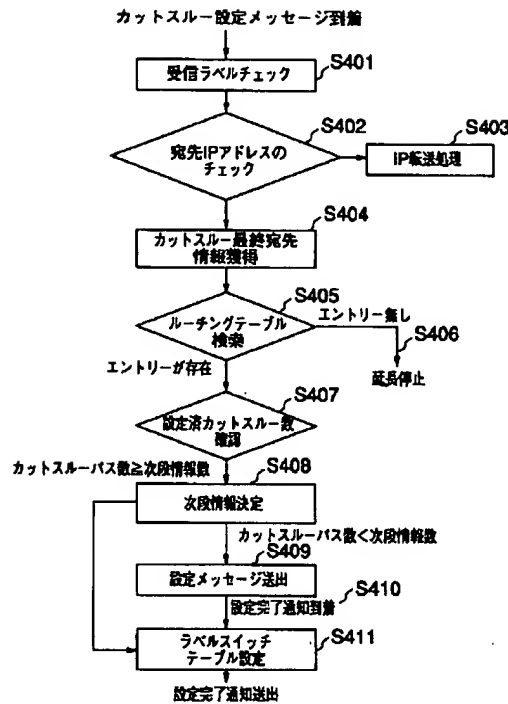
【図7】

701 受信ラベル	702 出力インターフェース	703 送出ラベル値
⋮	⋮	⋮

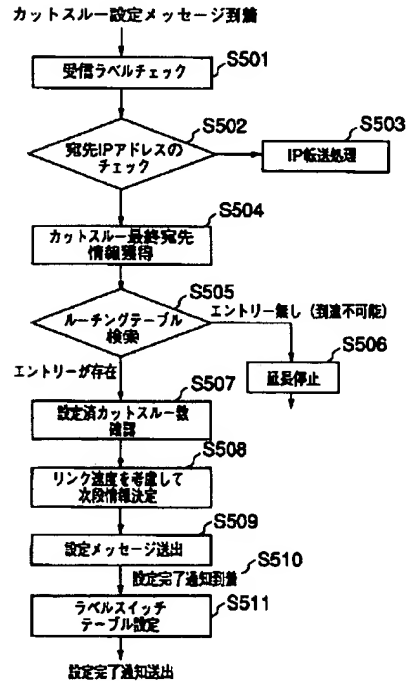
【図3】



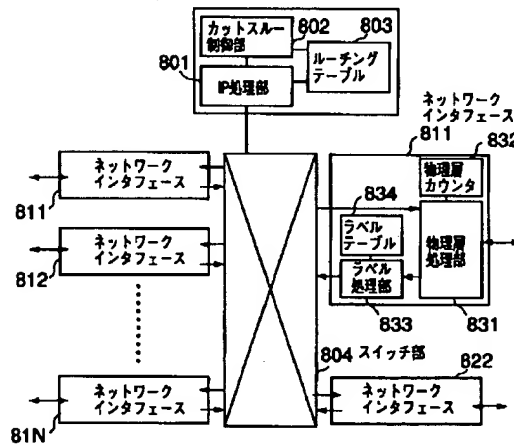
【図4】



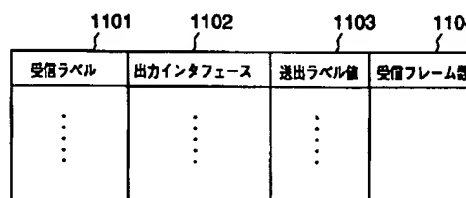
【図5】



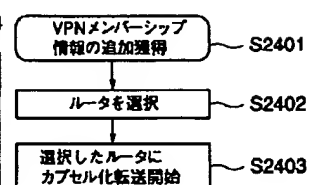
【図8】



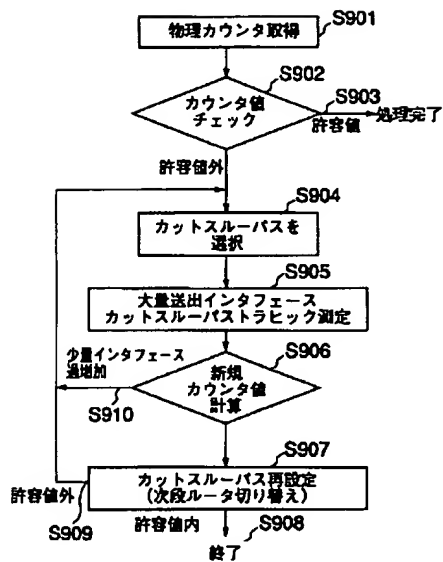
【図11】



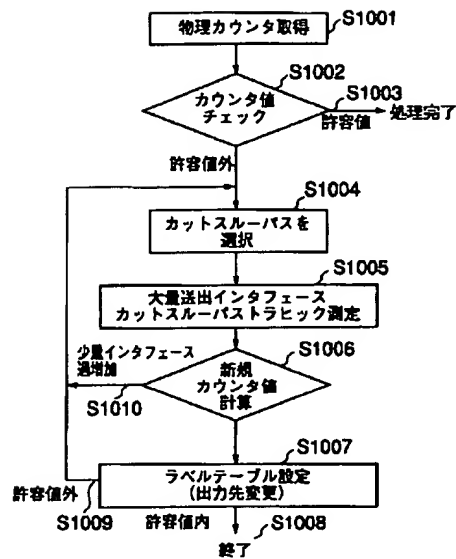
【図24】



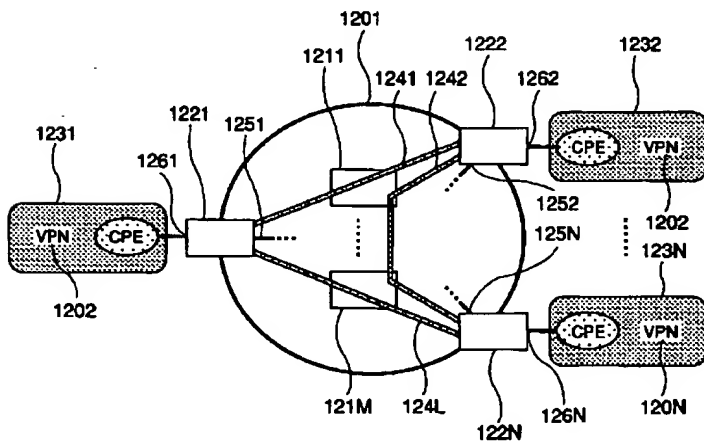
【図9】



【図10】



【図12】



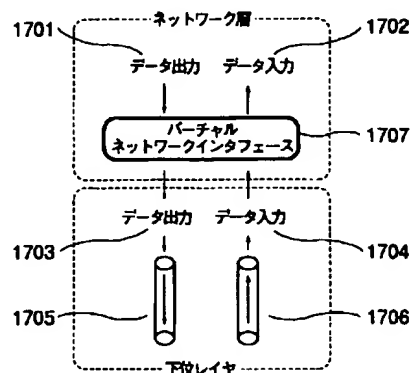
【図16】

1601 VPNフロー識別子	1602 LSPのラベル値	1603 パスの識別子
...

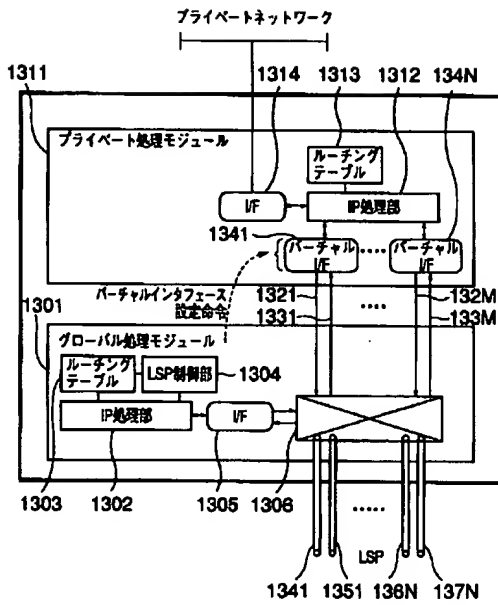
【図15】

1501 VPN識別子	1502 プライベートアドレス	1503 グローバルアドレス
...

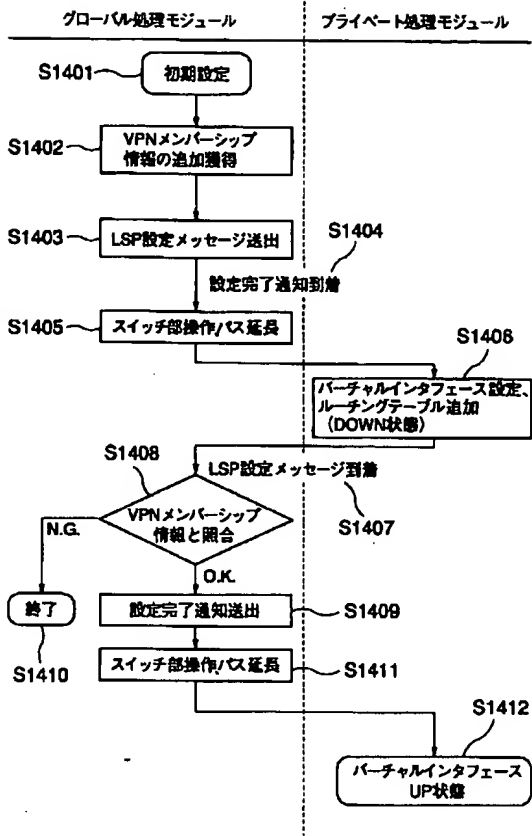
【図17】



【図13】



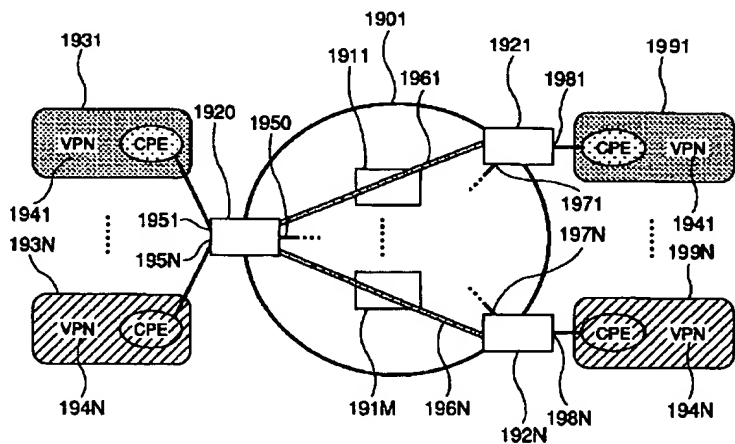
【図14】



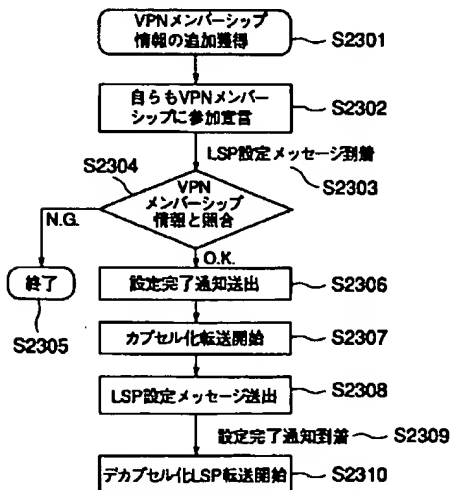
【図18】

宛先	次段情報	状態	インタフェース名
...

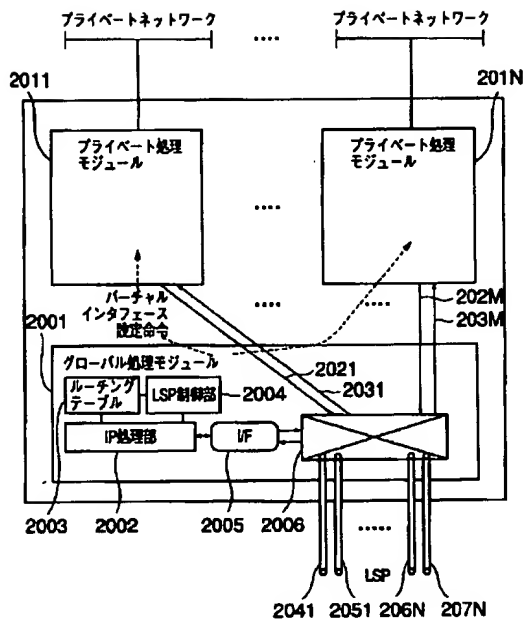
【図19】



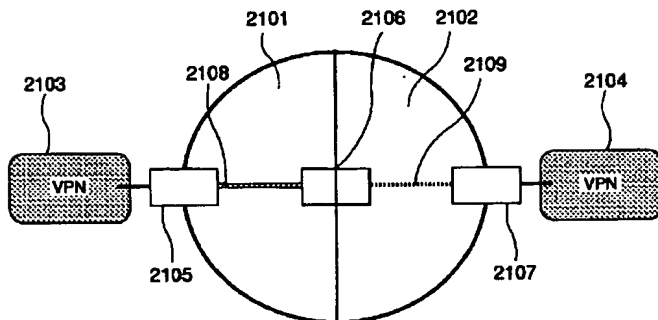
【図23】



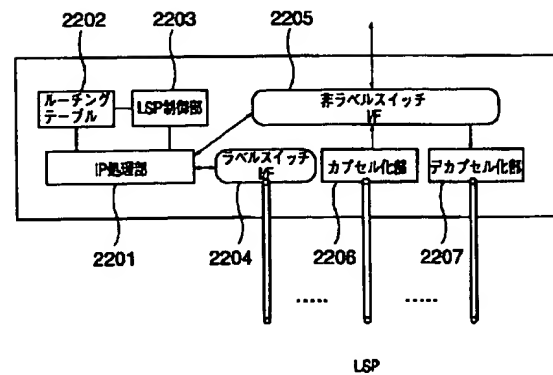
【図 20】



【図 21】



【図 22】



フロントページの続き

(72) 発明者 茂木 章善
東京都日野市旭が丘 3 丁目 1 番地の 1 株
株式会社東芝日野工場内

F ターム(参考) 5K030 GA13 HA08 HC01 HD03 JT06
KA02 KA05 LB05 LC11 LE03
MA01 MB16
5K033 AA03 CB06 CB08 DA01 DA06
DB03 DB12 DB14 DB19 EC04